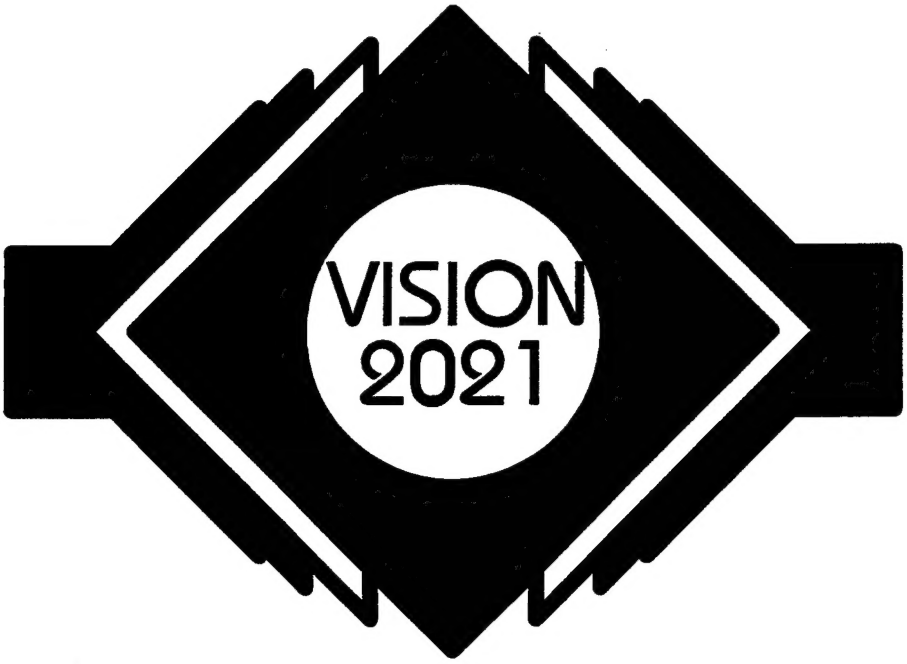

SECURITY ISSUES
for the
NEXT QUARTER CENTURY

PROCEEDINGS

Edited by Theodore R. Sarbin, Ph.D.

June 25-26, 1996
BDM Federal Headquarters
McLean, Virginia

Sponsored by
Defense Personnel Security Research Center
and
Security Policy Board Staff

TABLE OF CONTENTS

CONFERENCE PROGRAM

TUESDAY, JUNE 25

0830 Registration, coffee

0915 Introduction
Theodore Sarbin
Conference Coordinator

Welcome
Roger Denk
Director, PERSEREC

SESSION I

0930-0945 *The Future of Information Security*
Emmett Paige, Jr.
Assistant Secretary of Defense, Command, Control, Communications and Intelligence (C3I)

0945-1015 *Dramas of Control: Consequences of Electronic Security on Organizational Loyalty*
Peter Manning
Professor of Criminal Justice, Michigan State University

1015-1045 Break

1045-1115 *Information and Power: New Views, New Implications*
John Arquilla
Associate Professor of National Security Affairs, Naval Postgraduate School

1115-1200 Discussion of Session I papers
Discussant: Michelle Van Cleave
Attorney, Feith & Zell

1200-1330 Luncheon

SESSION II

1330-1400 *Torment of Secrecy Revisited*
Eric Biel
Staff Director, Commission on Protecting and Reducing Government Secrecy

1400-1430 *The Need for Secrecy Reform*
Steven Aftergood
Federation of American Scientists

1430-1500 Break

1500-1530 *The Intelligence Community: The Next 25 Years*
Douglas Perritt
Principal Deputy, Information Warfare, Security and Counterintelligence, ASD/Command, Control, Communications and Intelligence

1530-1615 Discussion of Session II papers
Discussant: Scott Armstrong
Executive Director, The Information Trust

1615 End of Session

WEDNESDAY, JUNE 26

0845 Coffee

SESSION III

0915-0945 *Personnel Security: Now More (Important) Than Ever*
Maynard Anderson
Arcadia Group Worldwide, Inc.

0945-1015 *Security: Another Perspective (tentative title)*
Seymour Hersh
Journalist

1015-1045 Break

1045-1115 *What Can We Protect in the 21st Century?*
Harry Letaw, Jr.
Chairman and CEO, Essex Corporation

1115-1200 Discussion of Session III papers
Discussant: Ethel Theis
Associate Director, Information Security Oversight Office

1200 Luncheon

SESSION IV

1330-1400 *Security: Making it Work through Reciprocity*
Peter Saderholm
Director, Security Policy Board Staff

1400-1430 *Economic Espionage: Looking Ahead*
Kenneth Geide
Unit Chief, Economic Espionage, FBI

1430-1445 Break

1445-1515 *Future Security Technologies*
Dan Smith
Program Manager, Technology Development Program, Office of Safeguards and Security, Department of Energy

1515-1600 Discussion of Session IV papers
Discussant: Linton Wells II
Deputy to the Under Secretary of Defense (Policy) for Policy Support, Office of the Secretary of Defense

The statements and opinions of the conference participants have not been approved by the Department of Defense and are not necessarily in accordance with Defense Department or U.S. government policy. Each participant is responsible for his or her own remarks, including any errors in them. No corrections have been made in any statement of any participant.

INTRODUCTION AND WELCOME

THEODORE R. SARBIN

Dr. Sarbin joined the faculty of the University of California, Berkeley in 1949. He served 20 years at Berkeley before moving to the University of California Santa Cruz campus. Since 1976, he has been Emeritus Professor of Psychology and Criminology.

Dr. Sarbin joined PERSEREC in 1987 as a research psychologist. In 1991 he wrote a report on homosexuality and personnel security. Since then he has completed a number of position papers for PERSEREC, including *The Moral Climate of Trust and Betrayal; Identifying Personnel Susceptible to Committing Computer Abuse and Crimes; The Power of Resentment; A Criminological Approach to Computer Crime*; and *Sabotage and Espionage in the Computer Age*. He is co-editor and contributor to the book, *Citizen Espionage: Studies of Trust and Betrayal.* His current research interests at PERSEREC include developing proposals to reduce the frequency of computer crime and abuse, and conducting research to help in understanding the trust-betrayal features of citizen espionage.

THEODORE R. SARBIN, Conference Coordinator

As the coordinator of this conference, it is my role to provide a preface to *Vision 2021*. The initial plan for this conference was developed following a PERSEREC-sponsored intensive workshop that dealt with the "peopleware" aspects of computer crime. One of the unexpected consequences of that project was the clear recognition that the bureaucratic separation of information security from personnel security rested on a false dichotomy. However useful such separation might have been in times past, continuing to act as if information security and personnel security belonged to unrelated domains can lead only to counterproductive outcomes. Whatever hardware and software technologies are invented to maintain the integrity of information, in the final analysis, it is *people* who violate security rules. As will become evident during the 2 days of this conference, we have avoided employing that false dichotomy.

As a nation, we have lived through various historical stages, such as the age of railroads and the age of industrialization. We are now living in the age of information. The microchip has changed the world; its use facilitates the rapid flow of information on a world wide basis. One result of the increase in information flow is the creating of a global village. For the global village of the 21st century, national boundaries are becoming less and less relevant.

Because our energies are so often directed toward developing practices and procedures to implement security policies, we are likely to overlook the fact that--in the main--the implicit meanings of information security and personnel security center on protecting secrets. Information security experts have directed their efforts to keeping secret information from our adversaries; personnel security experts have devised procedures for selecting and educating personnel who would hold government secrets inviolate. History tells us that these practices were only partially successful. Despite the best efforts of information and personnel security specialists, secrets have been purloined and delivered to agents of foreign nations, often by trusted government personnel.

Continuing the use of the global village metaphor, it is a commonplace that villagers cannot keep secrets from prying neighbors. Given the increased use of computer networks, it is legitimate to ask whether it will be possible in the 21st century to maintain the levels of secrecy that characterized government practices during the past 50 years.

We organized *Vision 2021* around the theme that we are heading straight into the information age. Our goal is to raise the consciousness of policymakers in government and industry to the necessity for looking ahead, to recognize that the bureaucratic formulae of the Cold War may be largely irrelevant to the age of information. To this end, we selected speakers from government, from the private sector, and from academe, each of whom would help illuminate the misty paths into the uncertainties of the next century. It is our hope that your attendance at this conference will stimulate you proactively to explore with your colleagues the national security implications of living and working in the age of information.

ROGER DENK

Dr. Denk spent 20 years with DIA, ending in 1987 as Chief of Public Affairs and Declassification. His DIA career included tours in directorates of both current intelligence analysis and operations. He was graphics and security review editor of the first three editions of *Soviet Military Power.* He edited intelligence chapters in the *Statement of Military Power of the Chairman, Joint Chiefs of Staff* and the *Annual Report to the Congress of the Secretary of Defense* from 1979 to 1984. He is the author of over 300 intelligence publications.

In 1987 Dr. Denk joined PERSEREC as a research psychologist. In that capacity he managed research projects in the areas of personnel reliability, continuing evaluation, due process, and special access programs. He became PERSEREC's director in April 1989. He is responsible for the operations, programs and budget of PERSEREC, including acting as principal spokesman for the Center and serving as liaison to intelligence community groups and committees, and to industry.

ROGER DENK, Director, PERSEREC

Welcome to *Vision 2021: Security Issues for the Next Quarter Century*. This conference is sponsored by the Defense Personnel Security Research Center (PERSEREC) and the Security Policy Board Staff.

As Dr. Sarbin has just mentioned, the conference is an attempt to pause for 2 days and think about the future of security: what will happen in the next 25 years. We have invited a broad range of participants from government, the private sector and the press to help us deliberate this topic.

We have divided the conference into four Sessions. Three speakers will make presentations in each Session, followed by a discussant who will attempt to integrate the presentations. The discussant will then take questions from the audience directed to him/herself or the three speakers. This unclassified conference is to be recorded and the major presentations eventually published in a Proceedings. We hope to have as much dialogue as possible among the varied audience members and our speakers and discussants. I shall be introducing each speaker or discussant with brief biographical notes.

Before we begin, I would like to express appreciation to the staffs of both organizations sponsoring this conference, PERSEREC and the Security Policy Board. In particular I would like to mention Suzanne Wood at PERSEREC and Jim Passarelli at the Policy Board who worked closely together to develop the logistics for the conference and who will review the Proceedings. This has been a good exercise in interagency cooperation and I am grateful to Ms. Wood and Mr. Passarelli for their contribution.

SESSION I

EMMETT PAIGE, JR.

General Paige, this conference's keynote speaker, has been Assistant Secretary of Defense for Command, Control, Communications and Intelligence since May 1993.

He has had a long and distinguished career in the military. Enlisting in 1947, he received his commission in 1952. After serving in Vietnam, he was promoted to Brigadier General in 1976 and given command of both the U.S. Army Communications-Electronics Engineering and Installation Agency at Ft. Huachuca and the U.S. Army Communications Systems Agency at Fort Monmouth, NJ. Receiving a second star in 1979, General Paige commanded the U.S. Army Communications R&D Command and, in 1981, the U.S. Army Electronics R&D Commanded in Adelphi, MD. On his promotion to Lieutenant General in 1984, he took command of the U.S. Army Information Systems Command.

Following his retirement from the military in 1988, General Paige served as President and Chief Operating Officer of OAO Corporation, an aerospace and information systems company in Greenbelt, MD.

THE FUTURE OF INFORMATION SECURITY

Emmett Paige, Jr.

Ladies and Gentlemen, I am grateful for the opportunity to participate in this important conference. Few issues are more critical for our national survival than the protection of government secrets. I welcome the efforts of the sponsors of this conference to raise critical questions about the security programs that--even during the Cold War years--were only partially successful. Because we live in a crisis-oriented environment, our planning tends to be short term. *Vision 2021* is intended to raise the consciousness of policymakers to security issues in the rapidly changing political and technological worlds, and to the effects of these changes on the handling of secrets. In organizing this conference with its futurist theme, the Personnel Security Research Center (PERSEREC) under the leadership of Roger Denk, and the Security Policy Board (SPB) headed by Peter Saderholm, have undertaken an initiative of great importance.

As a fitting introduction to this Conference, I wish to share with you my views on some of the challenges we face to support today's warrior and the warfighter of the future, the changes precipitating these challenges, and our vision and road map to meet them. As the memories of the Cold War continue to fade, we are confronted by the stark realities of a global environment plagued with a new range and variety of threats likely to pose significant problems for us well into the 21st century. Regional conflicts in the Middle East and in the Balkans are examples of recent threats to regional peace and stability. Nuclear, biological, chemical and conventional weapons throughout the world are proliferating at an unprecedented pace. These capabilities are also potentially available to countries we would never have thought interested, let alone capable, a decade ago.

A wider spectrum of contingencies, including operations other than war, such as humanitarian and peacekeeping missions, has changed the way in which our forces may be employed throughout the world. New operational locations and environments require us to think about new ways to deploy and employ forces. The Department of Defense is reshaping and refocusing itself to handle all these changes, but the challenges are great. Against the backdrop of an uncertain global environment and evolving technologies, we find ourselves driven to re-examine missions, doctrine, and required capabilities on a more frequent basis. I see this Conference as a significant forum for re-examining one of these missions--the structure of secret-keeping.

One of the greatest challenges to creating a new information system, whether to support warfighters or to manage communications, is how to maintain security of information. Now with the administration's National Information Infrastructure (NII) initiative we have even greater challenges in this area. The vulnerability to government networks is increasing as data flow is simplified. The ability of individuals to penetrate computer networks and deny, damage, or destroy data has been demonstrated on many occasions. The most recent examples have been the well-publicized intrusions on the

Internet. The GAO estimated that last year Defense may have been attacked as many as 250,000 times.

Extrapolating into the future is an enterprise not limited to the development of warfare technology. To remain competitive in the global village, we must call upon the best minds to help us examine societal, political, and technological trends. Such an examination will be an aid to the formulation of policies for identifying what information should be clothed in secrecy and also to the development of practices appropriate to protect such information.

Some of the papers to be delivered over the next two days question the arbitrariness of the bureaucratic separation of information security (the technology for protecting secrets) from personnel security (the procedures for selecting and educating personnel entrusted with secrets). Whether stored in approved filing cabinets or on computer disks, secrets do not get up in the middle of the night and walk into a foreign embassy. People, men and women with legitimate or illegitimate access to controlled information, are the responsible agents who commit acts that compromise government secrets.

When we look at the modus operandi of American citizens who attempted to deliver secrets to foreign powers during the Cold War, it becomes clear that they were working in a culture in which information was written or printed on paper. The problem for the spy was to create a means to carry out the high risk task of purloining and transferring pieces of paper. The problem is different in the computer age: most information is stored in computer networks. The disgruntled employee sitting at his or her keyboard is in a position to copy secret information, to modify it, even to engage in sabotage by infecting systems with viruses, logic bombs, and other devices. We must look ahead and prepare for a world where every computer is in effect connected to every other. Are passwords and encryption adequate to protect vital information if authorized users with decryption codes prove to be untrustworthy? Or if hackers and crackers rise to meet the challenges of increasingly sophisticated computer technology?

The information revolution is influencing far-reaching changes in the way individuals communicate one with the other, in the way commercial transactions are conducted, in the way crises are managed, and even the way nations engage in warfare. Our ability to provide for the common defense is dependent on our ability to exploit the benefits of the information revolution at the same time managing the dangers inherent in rapid technological change.

We are dealing with a task of monumental proportions. Consider for the moment the impact on the ordinary citizen of disruption or loss of mortgage records, bank accounts, employment history, automobile registration, educational achievements, and what the loss, wrongful disclosure, or corruption of that information would entail in terms of invasion of privacy and quality of life. Keep this ordinary citizen scenario in mind and compare it with the following illustrations of "the information warfare threat." A recent

attack on a DoD information system transited nations in Europe, South and Central America, Asia, and, in a matter of milliseconds, found its target in the Eastern United States. Countering this speed-of-light attack is the fact that legally to pursue--not prosecute--just pursue the perpetrators across cyberspace, a search warrant is required by law. The magnitude of the problem becomes immediately apparent when we consider the time required to obtain a search warrant. It goes without saying that cyberspace criminals can continue to inflict damage during the delays involved in obtaining a search warrant. Those officials responsible for pursuing cyberspace criminals will always be faced with the legal/moral question: given that untold damage can be wrought in a matter of milliseconds, can we afford to wait for the issuance of a search warrant?

The future or our ability to maintain our national identity--at the same time preserving individual rights and freedoms--will be shaped by how effectively we can deal with limitless virtual entities and methods of attack that are being created by technological change.

To retain our leadership position, the security community must provide, consistent with law, the tools necessary to engage these virtual threats simultaneously on all fronts--personal, commercial, and national.

Our growing dependence on increasingly sophisticated and globally available information technologies creates vulnerabilities that can be exploited by any individual, group, or nation in cyberspace. The millions of computers connected to the global information infrastructure have dramatically increased the availability of computers as weapons as well as the potential to inflict significant damage on our nation's communication systems.

These vulnerabilities exist daily on information and data systems throughout the nation and can manifest themselves at any time and any place--from the personal computer used at home or in the workplace to the supercomputers of the scientific community to flight control systems that help insure the safety of commercial and military aircraft. These cyberspace vulnerabilities serve as silent reminders that such metaphors as *fortress America*, *sanctuary*, and *geographic isolation* are no longer useful in today's world.

Unprecedented is the herculean task of protecting all of the nation's electronic communication systems from unauthorized access, manipulation, corruption, and denial of service. It is estimated that the department of Defense provides end-to-end control of only five percent of its communications. The remaining 95 per cent rides the public switched networks--networks over which the Department of Defense has little control. Military defense systems depend heavily on the availability of timely and accurate information. Increasingly, that information is transiting the relatively unprotected, globally interconnected, public switched networks.

As the GAO noted, "Internet connections make it possible for enemies armed with less equipment and weapons to gain a competitive edge at a small price. As a result, this will become an increasingly attractive way for terrorist or adversaries to wage attacks against Defense."

We cannot overemphasize the need for awareness of security vulnerabilities. Awareness of the threats posed by information warfare has already demonstrated the need for security products, procedures, practices, and training to protect our information systems and infrastructure from both internal and external attack.

We must also continue to pursue research and development of technical and procedural solutions to protect our information systems, including applications that can detect attacks and formulate appropriate responses. We must be ready to employ new innovative security products from firewalls to virus checkers to the multilevel information systems security products of the National Security Agency.

We also need to be aware that these technological changes will also change our institutions. More information will be disseminated through all levels of our institutions and more people will be tempted to divulge restricted information to unauthorized recipients. The half-life of vital information will be much shorter than today because the ability to control access will be curtailed.

Looking into the future, we can expect that government requirements and increasing demand for commercial and private information security solutions will stimulate market forces to provide higher levels of information protection and personal privacy.

The participants in this conference will raise questions about the security implications of changing geopolitical and domestic events. Will a penetrating re-examination of the whole fabric of national secrets impact on the policies and practices of entrenched government bureaucracies? Given the recognition that government and contractor employees are fast becoming adjuncts to the impersonal flow of automated information, will the characterization of certain information as "secret" have the power to inhibit employees from unauthorized use of such information? We must address more vigorously than before "peopleware issues" as well as software and hardware issues.

We are truly participants in the age of information. We are successors to the recently terminated age of the Cold War. We cannot afford the luxury of focusing exclusively on finding ways and means of improving on policies and practices that might have been appropriate for the last generation.

The participants in this conference will make clear that we cannot rest in our efforts to deal with a continuous information warfare threat to the nation's security and our unique quality of life. The competitive race for information is no greater challenge than those faced by previous generations of Americans who were called upon to solve

apparently insurmountable problems. It was largely a social climate that encouraged innovation and technological expertise that made information warfare possible. It is this same social climate that fosters such enterprises as *Vision 2021* to encourage the formulation of critical perspectives on information and personnel security issues.

PETER MANNING

Dr. Manning is Professor of Sociology and Criminal Justice at Michigan State University. He has also been a visiting professor at SUNY, Albany; MIT; and the University of Victoria. He is the author and editor of some 12 books and numerous articles and chapters in scientific publications. He currently edits The Security Annual, is deputy editor of Justice Quarterly, and serves on the editorial boards of seven other journals. His research interests are in occupations and organizations, and medical sociology and criminology. His recent research examines legal decision-making, nuclear safety regulation, and private security.

DRAMAS OF CONTROL: SOME ANTICIPATED CONSEQUENCES OF INFORMATION TECHNOLOGY ON LOYALTY[1]

Peter Manning

INTRODUCTION

The introduction of electronic means of communication has been widely hailed as an "information highway" and seen generally as a felicitous augmentation of social life, especially worthwhile in large organizations (see dissent in reviews by Fallows, 1994, 1995). Little has been written on the consequences of electronic communications on teamwork, organizational loyalty and commitment. These are two dimensions of organizational engagement.

I define loyalty as a willingness to give more than is asked to the organization--time, energy, leisure activities with coworkers, and unpaid work on behalf of the company. Loyalty taps the socio-emotional dimensions of commitment, the felt or cognitive obligation to remain in a given organization. Loyalty and commitment can vary independently since a person can be quite loyal and uncommitted, very committed yet disloyal, both disloyal and uncommitted and so on. Disloyalty is the expressive dimension, commitment the structural dimension, of organizational engagement.

In a previous paper, I analyzed organizational loyalty, or what might be called "the loyal self" (or selves), in the context of corporate security (Manning, 1995). Organizations clearly generate quite different levels and even kinds of loyalty (Adler and Adler, 1988). In general, a loyal self maintains a degree of self-investment, belonging, and a positive emotional attachment to an organization. The loyal self is a context-based idea, shaped by the organizational culture and the sub-cultures in which one works. The introduction of information technology as a means of communication, surveillance, evaluation and control adds a new aspect of loyalty and may pattern future loyalty and commitment. In this paper, using a dramaturgical perspective, I consider the extent to which information technology might shape future work and related organizational loyalties. The issue of commitment is only obliquely addressed here.

---

[1] The presentation was accompanied by a set of visuals that summarized the main points of the talk. Please do not cite or quote without the author's permission. Dr. Manning is grateful to Michael Morris for his comments on a earlier draft and for suggestions and materials he used in the verbal presentation.

THE DRAMATURGICAL PERSPECTIVE

The dramaturgical metaphor is a product of recent trends in social life. It both reflects our times and captures many of its key themes and nuances. Rather than seeing social life as composed of rational, self-satisfying actors, as does economics and most of psychology, as variously structured political contexts for power-seeking, or as a class-based cage of exploitation and misery, dramaturgical sociology sees life metaphorically, as if it were a theatrical performance in which semi-scripted roles are played (Goffman, 1959; Burke, 1962; Brissett and Edgley, 1990).

Dramaturgy assumes that actors are required to make sense of situations with strangers in complex societies wherein many interactions are fleeting and snapshot-like, and reigning moral standards are vague, tenuous or ambiguous. In such a society, civility, loyalty and deference are likely to be situationally based, rather than rooted firmly in history or tradition. Interpersonal trust as a result is minimal, and little can be known directly about a person's character, intentions, life history or biography. Dramaturgy assumes that modern life is lived through and by inference.

Interactions are based on impressions. The sociologist Erving Goffman (1959) argues that much must be inferred indirectly from impressions given off, or captured in passing, rather than from what is directly given, because people understand that much interaction is like an information game in which actors artfully conceal and reveal intentions. Interaction is more like a puzzle or game than an unfolding story.

Dramaturgy, a framework for the analysis of interaction, directs attention to the ways in which patterns of communication selectively sustain definitions of situations (a coded or schematic picture of social meanings). In much the same way that plays are performances systematically staged to convey artistic impressions, social life is a process of selective presentation to maintain a working consensus about "what's going on here?" This focus creates and sustains the basis for social dramas. Actors, a concept used to refer to persons, groups, and organizations, perform using fronts (constituted by social setting, appearance, and modes or styles of interacting) to convey impressions to an audience. These performances may involve variously attempts to dramatize, sustain realization of the impression conveyed, idealization, mystification, and expressive control.

Think of policing, for example, as a performance. It is realized by use of fronts, props, costumes, and equipment, played out as a conscious effort at control in public settings, and conveyed situationally in a distant and authoritative manner. It is idealized by an ideology that claims policing is a "thin blue line" that protects life and limb, and employs the moral sanctioning of the law. Characteristic role repertoires, or routines, are associated with the police role, and these cue and stimulate audience expectations. Police strategies and tactics of interaction, used to control audiences, emerge from the constraints of teamwork and joint performances. Importantly, as an occupational group, police are constrained by societal expectations in the form of a mandate (Manning, 1977).

Social interaction, however, is not simply or even exclusively a strategic game (Goffman, 1969). It has moral dimensions. Both information control and control of (ritual) contact is required to carry off an impression successfully. "Failure to regulate the information acquired by the audience involves possible disruption of the projected definition of the situation; failure to regulate contact involves possible ritual contamination of the performer (Goffman, 1959:67)." Errors, either informational or expressive, can damage a performance, the performer, or both.

Performances before an audience imply that cooperation between performer and audience is required--even staging a fight requires mutual cooperation- as is teamwork by those who cooperate to maintain a projected definition of the situation (Goffman 1959:79). The quality of engagement with teammates is subtle. Teammates are reciprocally dependent and familiar with each other: [a teammate is] "someone whose dramatic cooperation one is dependent upon in fostering a given definition of the situation." (Goffman, 1959: 79). While teammates can easily misrepresent themselves to others, they will be hard-pressed to sustain this misrepresentation amongst themselves (Goffman, 1959: 82-83). Teammates differ in trustworthiness and control over the collective performance, and are mutually obligated to avoid "false notes," follow the team's definition of the situation, and avoid punishing teammates before an audience. In a sense, the fear of the stigma for performance failure, or "letting down the side," binds interactants to (even) situational proprieties.

The study of teamwork, how an interactional definition of the situation is maintained, is essential to the analysis of social organization. Teamwork links interactional sequences to self, on the one hand, and social structure, on the other. Teamwork and organizations are interrelated because organizations are bounded interactional contexts within which actors perform routines that in time build up roles and selves. Through repeated routines before audiences, performers can invest self in a role. Caution is needed here, because just as people's situated cominglings are transient, adequate to the moment, a role or position sufficient to carry off a performance is insufficient to accomplish more than the requirements of the performance. Situational requirements for interaction do not imply mutual orientation to a shared goal or mutual purpose (Goffman, 1959). Interactants are bound to do more than cooperate for situational management if they wish to achieve a goal. Rather than goal-achievement, team members rather more commonly attempt to produce the impression that they are achieving ends and serving official policies (Goffman, 1959: 250-1). This suggests that overt compliance and loyalty differ.

Loyalty to an organization requires something more than feelings of obligation to team members or audiences. In this sense, dramaturgy is somewhat unclear about the demands of organizational life on actors. On the one hand, dramaturgy emphasizes the ritual and ceremonial potential of each encounter, insofar as making a gesture or offering a partial self encourages reciprocity and deference. The importance of sustaining interactional proprieties is suggested by the several means to repair failures of such ritual encounters, such as apologies (Goffman, 1967). On the other hand, ritual ties are situational, a product of the interactional order, and their generality across performances is problematic even if teamwork comes into play.

Thus, dramaturgy alerts us to the fragility of long-term obligations and commitments, and the immediate power of situational exigencies. The morality of an engagement is the morality of the moment, and standards of lying and deception are based on the audience's tolerance for such performances. Further, this morality is predicated upon face to face communication.

Insofar as mass media and information technology alter the character of interpersonal communication, they must be considered as factors in the shaping of loyalty and commitment.

CHANGES IN SOCIETY AND MEDIA

Increasingly, interpersonal processes are mediated. Large chunks of modern experience are derived from or based upon electronically represented images rather than exclusively from direct, sensate personal experience (Poster, 1990). Clearly, these changes have implications for organizationally based loyalty. The interposition of visual media alters the relationship between an audience and a performer once bound by mutually shared expressive burdens. New social realities (definitions of the real and the significant) are framed by media, and by computer screens which create complex and laminated social realities. Goffman was aware of the potential for a "symbolizing spiral" in which symbols reference other symbols and other symbolic worlds, creating a multiple and "laminated reality" (Goffman, 1974 pp.156-157ff).

Perhaps this is why Goffman (1974: 8) omits from his analysis (by implication) technologically mediated interactions. He rooted his framework in a fundamental baseline of primary reality, embodied face-to-face interaction (Phillip Manning, 1993).

Extensive and powerful mediated interactions now may shape organizational life as much as face-to-face experiences. On one hand, they sustain interactions unrestrained by time and space. Computers with screens enabling various forms of visual interaction, whether in the form of "surfing" the WWW, playing video games, or participating in bulletin Boards, FACs, MUDs, or other interactive sites, permit interactions to exist "stripped," free of specific settings, times, people or places (Meyrowitz 1985; Gergen 1991). Furthermore, this interaction can be carried out with code words, passwords, false or notional identities, or with no direct connection to a social role (identified by a work, family, or personal attribute). It is increasingly difficult to distinguish and mark the limits of these electronic realities or predict how they will shape interactional vicissitudes.

On the other hand, electronically mediated relations, organized around e-mail, the World Wide Web, pagers, cellular phones, and FAX machines, can create, enhance, sustain, and destroy relationships, and forge links between the otherwise distant and unconnected (Gergen, 1991, Rheingold, 1992). These relations range from quite intimate relations to business transactions and play, following one's curiosity across sites, hearing messages, watching videos, reading texts, or seeing amazing graphic displays. These changes in interpersonal relations, partially shaped by the media, affect manners and customs as well as

etiquette. They also affect the self-other dialogue in the sense that a murky, distant other dances on a screen or is known as a disembodied voice rather than a significant member of a proximal social world.

Selves, when linked to significant others who represent the moral consensus of a society, are conventionally viewed as the most powerful source of social control (Mead, 1934). The embeddedness of selves in social relations, with particular people in a particular time and space, serves as a powerful form of social control, because through the image of the generalized other, values, standards and rules of thumb symbolized, selves are self-regulating. Action is constrained both by immediate interactions leading to shared subjectivity and connections with others through symbolic ties and group obligations. Through interaction, the collective other, generalized sentiments or feelings for groups, arises, leading to generic subjectivity (Weick, 1995).

The introduction of mass media effects and the "stripping" of social relations would appear to vitiate formal social controls and moral restrictions associated with intimate private relationships. Visually mediated interaction, like watching a movie, may confound many conventional boundaries on interactions based on gender, age, race, and class (Meyrowitz 1985). Many cues used to establish trustworthiness, personal identity, non-verbal gestures and posture, and even deception and deviousness, are absent. Many cues to deception are absent.

In addition, modern media dissemble, fragment social worlds, intertwine genres (news+ drama = "docudrama"). Unlike the collective conscience (Durkheim, 1961) that links concrete interactions through practices with norms and values, modern media frame one sort of reality initially set apart from everyday life yet an intimate part of it in order to produce multiple and arbitrary social realities. They are crafted and stylized, and governed by media logic (Altheide and Snow, 1991) rather than grand integrating conventions such as religion or nationalism. Even symbolic communities, people linked only though electronic interactions, exist (Rheingold, 1992). Tensions exist in framing meaning because meanings can be located in various social realities, and easily changed by a change in context.

These changes in interaction and social control have central relevance to the analysis of contemporary organizational loyalty. Is this analysis consistent with the claim that we are seeing the emergence of an "information based society?" I now contrast these assertions about the importance of the interpersonal, expressive and emotional, and the visual, with an alternative (information-based) conception of society. The concept of an information-based society is misleading with respect to identifying issues in organizational loyalty.

AN INFORMATION-BASED SOCIETY?

Many have argued that the future will shaped by information, interacting with culture or economics (Poster, 1990). It is claimed that as electronically connected markets emerge, tight links will develop between buyers and sellers. Computer networks and attached PCs will tighten the loop between desire, expenditure, and possession. This will

lead to increased efficiencies because computer-driven consumption will reduce transaction costs and the externalities currently associated with market transactions. This increases productivity. Fewer workers will be needed to produce more goods and services and electronically mediated communications will facilitate distribution of goods, services, and information. Office work is more likely to be done in a virtual organization (Handy, 1995), at home, or on the road, through links to others via screens, computers, cellular phones, fax, e-mail and the WWW. Skill and information will be the basis for stratification, both horizontal and vertical. Interpersonal negotiations and meetings in a specific place are less likely. Freedom of choice and speed of electronic technology heightens individualism. This, in brief and perhaps unfair summary, is an information-driven model of future social relations.

However, there is good reason to believe that such forces seen as equalizing or even massifying, are not independent, but are rather corallaries of the current pattern of (inequitable) distribution of power and control (Lyon, 1994). Information is not a thing, but a symbolic matter fast becoming a commodity. Marx saw surplus value as organizing class relations, and information may become the new source of analogical power. Information will follow channels that maintain or even exaggerate the present stratification system. Lack of information access will further marginalize those without access. Power more likely produces information, not the other way around.

Recall that dramaturgy emphasizes the integration of various kinds of information, expressive and instrumental or pragmatic. A close reading of dramaturgical tenets would suggest that an "information-based society" is unlikely. Perhaps it is an oxymoron. An information-based system of vertical ranking of social groups, or stratification, must take into account the roles of both information (facts) and the significance they are given (meaning). Clearly, work will be shaped by the distribution of information, as will patterns of loyalty and deception, but the political process of meaning attribution is central to long-run change based on information technology (Manning, 1992, Thomas, 1994).

Below, I use dramaturgy to derive some propositions about information. These are stated baldly for purposes of argument.

1. Information, increasingly a commodity, is an emerging basis for organizing markets, not the least of which is an emergent market in information itself. Markets, including the information market, tend toward centralization (oligopsonic), even as other centripetal forces create pockets of disorganization and decentralization.

2. Information is one of the few commodities that can be stolen, transferred or copied without apparent trace of the crime.

3. When information is filtered, shaped, analyzed, and applied to decisions, it becomes valuable. The analysis process converts information or mere facts into meaningful material or data.

4. Information, and information about information- metainformation, the codes and processes by which information is transformed into data is in flux. It is increasingly becoming both centralized and decentralized. The analog here is encoding and decoding and software and hardware. These are patented by large market-controlling firms such as Netscape, Microsoft and IBM. Without the analytic tools, information remains mere information, not data or is so dispersed that it has little meaning. While some information is located in many accessible social spaces e.g., the WWW, with somewhat trivial consequences, information of strategic importance is controlled by a few people with control over metainformation. It can be argued that the attempt to control pornography on the Internet is less about pornography and more about the boundary threat of the Internet. The Internet permits "private play" at work and blurring of boundaries between work and play (M. Douglas, 1966). Efforts to control the Internet and to commercialize sites and access to sites, suggest that media giants will eventually control access to large segments of the working Internet. Control of the Internet by commercial interests replicates the structure of the aborted "computer revolution." While intended to decentralize information and democratize its distribution, it was soon tamed, shaped by mushrooming empires, and dominated by a few large firms such as IBM, Microsoft and Apple.

5. Learning and dentero-learning, or learning how to learn, or to change context to transform meaning (Bateson, 1972), are essential skills for maintaining a place in the vertical ordering of society. Deutro-learning enables people to select the kind of metainformation needed to produce or convert information to data. Extended learning, re-training, and education is increasingly privatized and commodified, sold and traded.

6. Those without the ability or willingness to learn, or without access to information processing skills and information, especially meta-information, increasingly will become marginal economically.

7. Information markets, now a part of national security concerns, will be shaped by the means used to create, monitor and regulate them. Social control will remerge as information control and surveillance.

In summary, information is interwoven with social values and meanings emerging from how it is used, who uses it, what it symbolizes to groups of people, and how people learn to understand and to use given information. These matters are social, not technological, and they form a part of dramaturgical realities.

TECHNOLOGY AND CONTROL IN WORK

The social patterning of technology applies as well to the introduction of an information technology into a work setting (Manning, 1992, 1992a, 1996). A number of

propositions about how information technology might shape work and loyalty can be deduced now. Information and expressive obligations interact in a complex fashion.

Insofar as information becomes a part of a cluster of key symbolic properties (that which is valued and can be bought and sold) controlled by an organization, collective dramas will arise. Collective dramas, or the display of symbols through stories, meetings and conferences, will mark and surround the control and dissemination of information. Information dramas, or dramas of control centering on acquiring, protecting, encrypting, and analyzing information, as well as stealing it, copying it, or fear of its loss, animate organizational processes. The CIA/Ames spy case is an example of an information drama. Information dramas provide warning signals of value to any intelligence system that intends to monitor loyalty. The problem about information dramas is that computer-based information has an ambiguous character to it--it is simultaneously "private," one's own information, and "quasi-public," the organization's. Where these boundaries are to be drawn is debated now in every organization. The screen reflects variously and simultaneously the self of operator and the face of the organization. Conversely, it is argued that workers should be protected against harassment on their "private screens"--an example here is the recent sexual harassment case won by a woman who was shown an offensive sex scene each time she booted up her computer and was judged correct in claiming the organization had failed to provide a secure work environment. Here are some propositions to be explored in my research.

Technology and organization interact over time (Manning, 1992; Thomas, 1994), each shaping the other.

If technology formats work ("informats," as Zubhoff (1988) terms it) and workers do not produce counterstrategies, information technology will lead to reinforcement of managerial authority on the basis of information control. Ambivalence to computer machinery, when linked to production and information about production (meta-evaluational information), will affect both workers and management. "Standardization," the MacDonald's effect (Ritzer, 1992), will shape work tasks in part by the informating effects of modes of computer communication, but computer formats are shaped in use by operatives. Police use of laptops, treating them as portable notebooks to be downloaded, introduces another step, linking mainframe to laptop, and may still require a trip to the precinct. Work routines still embed new technology. "Core" and "periphery" workers may emerge because the nominal (present) skills-base of an organization is ostensibly protected as organizations "downsize." While periphery workers are contracted--"outsourced"--core workers, connected to the central symbols, core values, and functions of the organization, are protected. This is a strong trend in the private security field, where guards, bar-coded inventory checks, and alarm systems are handled by short-term contract with large national security companies such as Pinkerton, Wackenhut and regional companies.

The need for trust, or loyalty based on inference alone, increases, but it takes new forms. It may be mediated by computer communication, or defined by organizational position rather than personal knowledge.

Ironies emerge because what is seen on a screen and what is known via past experience often differ. Supervision tends to base rewards and evaluation on one or the other.

This problem is characteristic of all formal tracking systems whether computer-assisted dispatch (CAD) in policing, navigational aids in aviation, or ship-based radar.

Interpersonal understandings, tacit agreements and unwritten agreements, the non-contractual aspects of contracts (Durkheim, 1960; MacCauley 1967), erode and recede in salience as face-to-face interactions are less necessary for long-term economic relations. Many expressive interchanges (interpersonal relations-gossip, office politics, friendships) shift to e-mail and the WWW; a folklore grows around mistaken communications and foul-ups. Meetings may focus less on information exchange and more on rituals of solidarity and expressive sharing.

If fewer face-to-face interactions serve as ontological anchors, pinning people down to obligations and audiences, new etiquettes and rituals must be devised to control mediated interactions (Marx, 1994). For example, consider the grammars of "hot lines" for computer support (Pentland, 1993), the "verbal menus" businesses use to screen calls or the ambiguous etiquette of answering machine announcements.

The social screens erected around people are electronic such as answering machines, a "voice mail box" and the irritating message "I am sorry, Mr Smith's voice mail box is full"; e-mail; and phone menus that distance callers from personal contact (even a human voice). To reach a human voice, one has to work through a series of options, and a "touch tone tango" results.

The demands of sustaining technical communication and competence may (ironically) reduce the power of face-to-face interpersonal relations. The police, for example, have clearly traded face-to-face interaction for technologically guided work e.g., dispatched work (Airline clerks balance it precariously, in my experience).

Virtual realities (those created on a screen), or cyber-realties (social worlds created visually as in video games, hypertext constructions, and fantasy games), and experienced realities may clash. They may be inconsistent or even patently paradoxical.

Interpersonal relations, once the nexus of a problem solution, are obviated, e.g., "...the computers are down and we can't respond to your problem now."

Multiple (fast) modes of communication with colleagues develop. Networks of collective action extend quickly and in erstwhile form beyond the organization via e-mail, WWW, faxes, express mail, and cellular phones. New lags and ambiguities in communication result.

New technologies mediate interactions e.g., "voice mail"; "e-mail"; answering machines; and faxes. Power-dependence (who owes what to whom when) is symbolized by lagged responses and patterned ambiguities in response.

Lack of deep knowledge of work practices and their abstract features means that managers may focus elsewhere to monitor workers, such as expressive matters of play, emotion, personal amusements, sex and gossip.

Therefore, one might expect increasing concern about employees playing video computer games, sending personal e-mail messages and using the phone for personal communication. Opposition is both symbolic and expressive.

Workers respond to technological changes by seeking detailed job descriptions and union contracts to stabilize control of their jobs (Zubhoff, 1988). Loyalty in this context means control of an individual job. Others, middle and top managers, will regard technological change as an information drama, a political battle over symbolic control and use of information (Thomas, 1994).

Managers emphasize wholism, or loyalty to the organization as a whole. While claiming they control their subordinates, they actually feel little control of their own work lives (Zubhoff, 1983). Zubhoff suggests that this results because managers lack the information or skill to do anything but "...surrender to the organization's purposes and values." (p. 404). Work processes are also a focus of control and surveillance. In abstracted-technical work, information about control processes can become a source of domination for managers and the basis for a power-dependence relation between workers and managers. Appropriated craft work knowledge in the paper-processing plant studied by Zubhoff (1988) became the basis for new forms of rationalized bureaucratic control.

A heightened, self-reflexive focus results from intense, repeated, screen-self interactions (Heim, 1995; Rheingold, 1994). The computer monitor or screen is a micro conflation of self and other, often personalized and named ("My computer" is an icon on my "Windows 95" screen). Quite apart from displaying the self writing and written across the screen, the computer memory contains diverse emotionally laden material--personal, intellectual, familial, and work-related bits (e.g., the ads in *Newsweek* for the powerbook explaining what celebrities kept on their hard discs). Work memory is increasingly visual memory.

Decentralization of authority and work facilitated by electronic connections requires coordination through shared meanings, working consensus and interactions even as the instrumental dimensions of communication are elevated. In short, information technology does not reduce the need for social integration and expressive interactions, it may increase it (Weick, 1995).

In time, within an organization, skill and knowledge may be inversely related to position or rank because of generational differences in computer skills and mastery. New modes of sensemaking of computer behavior result and are a core of office lore and sharing of problem-solving techniques (Barley, 1986; Weick, 1995). An oral culture develops around shared practices (Sackman, 1991, terms this "directory knowledge"). This interaction between information technology and work routines introduces new content that reshapes the oral culture of the workplace.

INFORMATION TECHNOLOGY AND SURVEILLANCE

Clearly, work routines, interactions and skills shape loyalty. They also shape assumptions about loyalty by those responsible in organizations for loyalty and security. Here are some possible implications of the above propositions on the relationships between information technology and surveillance and control.

To the extent that employees interact with their screens and become embedded in cyber-reality, they tend to be less rooted in the interpersonal relations of their team or occupational group. A reduced level and quality of face-to-face relations result. Weick (1995), writing on high-tech crises, suggests that talk and interpersonal negotiations are the vehicles by which meaning is pinned down. The example of police dispatchers is very relevant here. More discussion and probative questioning of a caller is needed in emergency situations e.g. "A man with a gun," rather than less because this is the only way an officer can place an ongoing event in context. Pass through time is far less important than producing the context of the event for the officer who eventually must attend the call.

Expressive interactions with the screen as an audience, seeing one's self, potentially deracinate the loyal self from local significant others. Thus, a concern is the potential withdrawal of loyal selves from the public interactive arena. One might expect or even predict a focus of supervisors on expressive behaviors of employees, playing video games, simulated sex games, using the internet, or engaging in interactive simulated conversations, because these symbolize emotional distance from the work role and suggests a lack of emotional investment.

The physical presence of an employee, given a developed information technology, is less and less likely (Handy, 1995). Assessing work performance may require modification of trust and ways to assess it. Trust issues become paramount in supervision and evaluation (especially in promotion), and the role of trust in transactions will be rethought given electronic mediation of market relationships.

Observed behaviors may be less available than inferred traces or indirect measures of performance. Traces (evidence in files, in computer memories, archived on a main frame) of work performance become the basis for evaluations more than observed behaviors. These traces may in turn yield contradictory evidence. Traces of time spent, for example, may be inversely related to performance and quality functions. Again, police dispatchers and patrol officers are monitored for their time "in service" and how many calls per hour they process.

Patrol officers are expected to respond to calls and return to service. (The irony is that being "in service" is actually being available for service, not working, or being in service. That is labelled "out of service"!) A focus on the means of carrying out the mission, response to calls for service, reifies and misplaces attention from the quality and content of the response given to the caller and how information assists the officer in subsequent problem-solving. Since no feedback is given to operators by patrol officers, efficiency not effectiveness is rewarded (Manning 1988).

Stylistic aspects of communications become relevant traces in work evaluations. Hackers have been traced by use of programming styles, modes of entering the computer field and characteristic techniques for misappropriation of data. Unanticipated monitoring of behaviors results (stylistics, information, relations, sources of information, leisure) results from computer use (open the "cache" or history file on your Netscape program). Unanticipated (and often unintended) monitoring of work behaviors results. Traces and unobtrusive measures become more relevant to performance evaluation. Police in a suburban location in Michigan, for example, use the number of requests for vehicle information as an indirect index of activity and can monitor the numbers called on the radio-telephone.

Anticipated and unanticipated evaluations are now available. Decisions about what behaviors are to be monitored and what will not be (or will be prohibited) require deliberation. What will be the focus? Will it be a) targeting (persons, places, or activities) b) general surveillance via video cameras and checks of computers; c) monitoring of specific indices of work performance?

Since work deviance in an electronic computer-organized work environment is likely to be hidden, symbolic, abstract, and not incident-driven, and is often in the grey area between the law, policy and common-sense morality, investigative tools and approaches (strategies and tactics) to crime prevention and detection must change. Auditing skills, computer science, and programming ability are required to investigate computer-based crime. Much deviance and crime in the work place, aside from workplace violence, will be process-crimes, not incident-driven crimes, and involve misuse or stealing of information.

This suggests that rather than developing systems of negative reaction and sanctioning, often with the criminal law, the focus in organizations will be increasingly on risk-assessment. This approach parallels an insurance model of predicting and managing risks rather than reacting to and punishing them. Associated with this move to risk assessment is increased restitutive (or remunerative) sanctioning rather than criminal sanctioning. The combination of risk assessments and restitutive sanctioning suggests that in future organizations should combine sophisticated intelligence systems with reactive surveillance and security systems (indications of violations that have taken place). Intelligence systems monitor, assess, and put in context signs (something that stands for something else in the mind of someone) or warnings of potential or actual loss of property, information and/or personnel.

Developing intelligence systems will require a re-orientation of the information base of organizations to enable decisions about competition and strategic planning. Further, intelligence implies active counterintelligence and of course, counter-counterintelligence. These systems are in themselves value-free, and organizational ethical standards concerning the gathering and use of information from competitors may be required.

Targets of surveillance will have to be differentiated. While external competitors are organized, and therefore the metaphor of military intelligence is relevant, "disloyal" employees may not be organized, act systematically, nor carry out coherent plans. These represent two distinct problems of loyalty. As has been suggested in the PERSEREC analyses of spies, the problems to which treason was a solution are often personal, financial or psychological and work and personal life situations were intertwined.

Finally, computer-based work may increase productivity and output, both deskilling some and elevating others. When combined with downsizing, firings, and attrition, information technology contributes to producing deracinated and angry once-loyal employees. For these workers, the computer and core knowledge are weapons or vehicles for revenge.

COMMENT

It appears likely that whatever the sources of employee loyalty within an organization, they will be altered in some fashion by the introduction of information technology. Dramaturgy suggests that current bases of loyalty are situational entanglements and constraints, obligations to teammates in the performance context, and repeatedly playing a role before a given audience. Impression management, a key skill in modern life and to deception, is facilitated when face to face interactions are reduced in frequency.

Information technology is patterned by social relations (Thomas, 1994; Manning, 1996) and in time, social relations are patterned by technology. However, since information technology changes the character of secrecy (what information is shared with whom), modes of protection required, social means for detecting risks, e.g., the intelligence systems in place, as well as techniques of transferring information and tracing such transfers, the nature of loyalty and disloyalty is in part based on information security. There can be no easy disconnection of people security and information security.

This discussion has implications for the analysis of security and security awareness. In the military, or in any organization in which deference to authority and vertical rank obtains, loyalty is based upon and indicated by deference to commands. In the professions, loyalty is assumed to be learned or present as a result of recruitment and high rewards. In the military and academe, loyalty taps work engagement and emotional attachment. In industrial organizations, loyalty is to a job and perhaps to one's workmates, while "higher loyalties" are rare and difficult to socialize. This is also true of the lower participants in any large organization. Few opportunities for mobility exist, spatial and temporal separation of workers and management persists, and little interaction exists between management and

the worker. Few ritual or ceremonial activities integrate segments, and security's core dramas, as enacted, generally further mark these existing differences. As Gordon (1996) has shown, the fat (management) are growing fatter (in wage terms) with no increase in productivity, while the lean (the workers) are being fired and being paid less.

The "loyal self" is contextual and may be even segment-specific. If we imagine three segments in workplaces, top management, middle management and workers, they are rooted differently in the organization. The loyalty of employees is based on their typically narrow commitments to the work, income, or workmates. Many are either alienated because they have little or no future, or because job security is highly problematic. Many hold only the most tenuous loyalty to the organization. They are often distrusted. This is why, in part, workers are subject to the surveillance and monitoring that may increase their distance from the organization. The loyalty of the lower participants is made more problematic by efforts of security to control, surveil, question and monitor their movements and activities. Their loyalty is judged by relative lack of negative indices, absences, turnover, loss by theft, and measured by more distant and abstract data, derived from monitoring, technological or electronic, via television, computers, and card-reading machines.

Management, middle and top, identify more with the organization, their careers, are seen as trustworthy, and receive many "benefits" denied workers.

The three segments are likely to come into contact with security differentially. They are suspected for very different sorts of trust violations. Different approaches are taken to discovery: top employees are investigated after allegations of misconduct are laid, while employees are actively and routinely monitored.

This leads us to an irony concerning functions and prestige, because establishing the worth of security in part is based upon maintained secrecy, confidentiality and privacy, and trustworthiness, rather than visible (negative) indices such as: thefts cleared, arrests, incidents reported, and dollars saved by staff reductions, "outsourcing," or technological innovations. The (potential) positive contributions of security to employees' social integration is overlooked. As security moves away from a narrow sense of detecting and punishing, it will want to consider ways to encourage social integration and performance. The symbolic cost of high management wages to corporate morale and to relative deprivation as source of discontent should be considered.

NOTES

1. Portions of this critique of dramaturgy have been adopted from Manning (1996), overstates for purposes of argument the passivity and dislocated character of the modern self, the fragility of social relations, and the irrelevance of science and history. While such schemes exaggerate, they nevertheless capture subtle, yet undeniable features of advanced societies. Trenchant truths, inferred and very prescient, are implied, if exaggerated, in these writings. Clearly, some of the assertions require empirical research and analysis.

2. The mass media, primarily television, now create and construct political events in which viewers are mere recipients of a discourse that weaves together and confounds everyday and symbolic realities. Constructed materials are created and presented as "facts" and "data" (Edelman 1988: pp.10-11). The media sustain a powerful canopy of meaning, semiotically speaking, that is based on signifiers without easily identifiable signifieds. In other words, the defining feature of "reality" is that which can be copied, reproduced, or become an "equivalent representation" (Baudrillard 1988, pp. 145ff). For example, police are now viewed on tv in news, as media figures, on dramas, documentaries, as figures in Rescue 911 and America's Most wanted, as entertainment manques on "Cops," and embedded in videos on news shows, CNN, etc.

3. While television certainly shapes actions, choices and justifications for conduct, the precise degree to which it does is unknown. The modification of the concept of reflexivity concerns cultural change, not merely individual choice.

4. For example, see a recent review of a number of books on computers in the *New York Review of Books* (February 15, 1996, XLIII). James Fallows, a journalist whose expertise is computers (See also *New York Review of Books*, March 1994)] assess Bill Gates' vision of the future.

5. Consider some rather incidental examples. 1) There is a tremendous increase in interest in "intellectual property," copyrights and control over means to access information as well as information itself. 2) Michigan State University recently established an Office of Intellectual Property and sponsored an on-campus seminar on intellectual property rights for faculty. 3) FBI has shown an interest in supporting industry by investigating loss of industrial secrets, including software and other technologies. 4) There is evidence of a shift in concern in the federal Government and private companies involved in security and intelligence from "conventional spying" to industrial espionage from the more than 50 countries now involved (Carter, 1996).

5) Academic resistance to converting ideas into property is eroded by the powerful workings of the law and lawyers. 6) Control of information and access to information remains central to vertical and horizontal stratification and to issues of loyalty in the future.

6. Information is used to create and manipulate desires. The commodification of desire, systematically extended by advertising by visual imagery, is produced and sustained by the decentralized network of information -the internet- which works by diffusing information throughout the network, rather than clustering it in a few controlled sites.

7. The paper draws on interviews with 12 heads of security in leading (innovative) American corporations, field work in one firm's corporate security division, and several long interviews with heads of security in three of America's largest corporations. I also draw on a survey carried out by the Michigan State University School of Criminal Justice.

LIST OF REFERENCES CITED

Adler, P and P. Adler 1988. "Intense Loyalty in Organizations," Administrative Science Quarterly 33: 401-417.

Altheide, D and R. Snow. 1991. Media Worlds in the Postjournalism Era. Hawthorne, N.Y.: Aldine/DeGruyter.

Barley, S. 1986. "Technology as an Occasion for Structuring," Administrative Science Quarterly 31:78-108.

Bateson, G. 1972. Steps Toward an Ecology of Mind. San Francisco: Ballantine.

Baudrillard, J. 1988 Selected Writings. ed. Mark Poster. Palo Alto: Stanford University Press.

Brissett, D. and C. Edgley eds. 1990. Drama in Life. Hawthorne, N.Y.: Aldine.

Burke, K. 1962. A Grammar of Motives and A Rhetoric of Motives. Cleveland: World.

Carter, D. 1996 "Security in Emerging Markets." Talk presented at conference on "Security in Emerging Markets," Michigan State University, May.

Douglas, M. 1966. Purity and Danger. New York: Pantheon.

Durkheim, E. 1961. The Elementary Forms of Religious Life. New York: Collier.

Edelman M. 1988. Constructing the Political Spectacle. Chicago: University of Chicago Press.

Fallows, James 1995. New York Review of Books, "Bill Gates' Vision" (Feb 15, 1996 XLIII).

Fallows, James 1994. New York Review of Books.

Gergen, Kenneth 1991. The Saturated Self. New York: Basic Books.

Goffman, Erving. 1959. The Presentation of Self in Everyday Life. New York: Doubleday Anchor.

Goffman, Erving. 1967. "Deference and Demeanor" pp. 47-95 in Interaction Ritual. Chicago: Aldine.

Goffman, Erving. 1969. Strategic Interaction. Philadelphia: University of Pennsylvania Press.

Goffman, Erving. 1974. Frame Analysis. New York: Basic Books.

Handy,C. 1995 "Trust and the Virtual Organization" Harvard Business Review. May-June: 40-50.

Heim, M. 1995. Virtual Reality. New York: Oxford University Press.

Lyon, D. 1994. The Surveillance Society. Minneapolis, Minn.: University of Minnesota Press.

Macauley, S. 1967. "Non-Contractual Relations in Business" American Sociological Review 28 (Feb.): 55-67.

Manning, Phillip. 1993. Goffman and Modern Sociology. Palo Alto: Stanford University Press.

Manning, P.K. 1988. Symbolic Communication. Cambridge: MIT Press.

Manning P.K. 1992. "Technological Dramas and the Police: Statement and Counter-Statement in Organizational Analysis" Criminology 3O (Aug.): 327-346.

Manning P.K. 1992a. "Police Information Technology" pp. 349-398 in Michael Tonry and Norval Morris, eds. Modern Policing. Chicago: University of Chicago Press.

Manning P.K. 1995. "Loyal Selves" seminar presented to PERSEREC, Monterey, California, October.

Manning, P.K. 1996. "Dramaturgy, Politics and the Axial Media Event" The Sociological Quarterly. 37: 261-278.

Manning, P.K. 1996a. "Police Information Technology: The 'Sailor' Phone." Information Technology 7 (March): 52-62.

Marx, G. 1994. "New Telecommunications Technologies Require New Manners." Telecommunications Policy. 18: 538-552.

Mead, G.H 1934. Mind, Self and Society. Chicago: University of Chicago Press.

Meyrowitz, J. 1985. No Sense of Place. New York: Oxford University Press.
Pentland, B. 1993. "Routines as Grammars of Action." Administrative Science Quarterly 39: 484-510.

Poster, M. 1990. The Mode of Information. Palo Alto: Stanford University Press.

Rheingold, H. 1992. Virtual Communities. New York: Harper Perennial.

Ritzer, G. 1992. The McDonaldization of Society. Thousand Oaks, CA: Pine Forge Press.

Sackman, S. 1992 Cultural Knowledge in Organization. Thousand Oaks, CA: Sage

Thomas, R. 1994. What Machines Can't Do. Berkeley: University of California Press.

Weick, K. 1995. Sensemaking in Organizations. Thousand Oaks, CA: Sage.

Zubhoff, S. 1988 The Age of the Smart Machine. New York: Basic Books.

JOHN ARQUILLA

Dr. Arquilla is associate professor in the Information Warfare Academic Group at the Naval Postgraduate School, Monterey, CA. He teaches courses on the history of special operations, international political theory, the revolution in military affairs, and warfare in the information age. He is author of *Deterring or Coercing Opponents in Crisis, Dubious Battles*, and *From Troy to Entebbe*, along with many articles and book chapters on a wide range of security-related topics. His current research focuses on the effects of the "control revolution," which will be examined in detail in his forthcoming book, *Society and Security in the Information Age.*

INFORMATION AND POWER: NEW VIEWS, NEW IMPLICATIONS

John Arquilla

Roger Denk's very kind introduction noted that I have some small knowledge of history--and I'll forewarn you that I like to look pretty far back. My book on the history of special operations begins with Troy, where two dozen Greek warriors and a very special piece of equipment (the Horse) infiltrated into the city and successfully ended that long war. My notions of cyberwar, which appear to have caught on a little bit in the last few years, began with the Mongols' use of Arrow Riders (a kind of Pony Express), and semaphore signal systems for relaying information. I think it is important for us to put a marker down to keep an eye on relevant historical precedents, even as we look ahead. Indeed, sometimes we look ahead by looking back first. I think Churchill put it extremely well when he said: "To assume that what is past is past is to surrender the future."

Ted Sarbin has invited me to talk a little bit about the future and I have decided to do so, giving special attention to the title of this meeting, *Vision 2021.* I know there are probably copyright or patent reasons for why that "1" is on the end; but, as I recall, 20/20 vision just means seeing at 20 feet what others see at the same distance. "2021 Vision" implies seeing things just a little differently. So think of me as that "1" in 2021--perhaps we'll see things from a different perspective.

What I would like to do today is to share with you a few of my thoughts on information and power--and how they relate to issues of national security strategy. I begin with a discussion of information in its various dimensions--that sees it becoming ever more material and quantitatively measurable. I'll give you three different views of information: as relating to the message conveyed, the medium of transmission, and finally the view of information as a form of matter with physical properties. In terms of power, a similar evolution has been occurring--but in the opposite direction--away from traditional, material-bound notions that originally focused entirely on physical resources. A second view of power sees that resources alone are not paramount; but that the way in which they are organized is crucially important. Finally, a third view is that power is becoming ever less material, or "softer," and grounded in ideas--like democracy.

Seen in this light, power flows in a cross-cutting current with information. As information becomes more physical, power becomes less so. Indeed, it is even possible that a kind of fusion of the two is going to take place. At the very least, the two are going to interact in unexpected and new ways in the future. The maximum view is that as Clausewitz put it, "knowledge will become capability." And so as not to forget our friends in Troy, let us remember Athena for a moment. She was the Goddess of Wisdom, a warrior who protected the state. Her image, the statue of the Palladium, had to be stolen by the Greeks, Virgil relates, before they could be sure that Athena would not provide the Trojans with the wisdom to understand what the Greeks were doing. Troy had to be

robbed of its symbolic fount of knowledge before it could be taken by subterfuge and force.

Let us consider this complex notion of information. And I should say, parenthetically, that, for those who have an interest in broad approaches to the topic, a chapter that I co-authored with David Ronfeldt of the RAND Corporation--upon which this talk is based--will come out in a book entitled *The Information Revolution and National Security,* published by the Center for Strategic and International Studies. It will be out this summer sometime, and is edited by Stuart Schwartzstein.

In any event, the least material form of information is what we began with--the spoken and written word. The spoken word, of course, goes back to our earliest human origins. Even in its least material form, information had a profound effect. The written word, for example, allowed complex, operational orders to be prepared, creating, perhaps, the first "revolution in military affairs." The great battle at Kadesh, fought over 3,000 years ago, was won by a smaller Egyptian army, in part, because the Pharaoh was able to give a set of detailed orders to his captains, which helped them to outmaneuver the Hittite hordes. Can you imagine giving orders in hieroglyphics? I can't, even though my notes *do* look like hieroglyphics!

The point is that, even very early on, information, not just the message, but also an advanced medium for its transmission, made a very great difference. Of course, moving from the written word to the telegraph to the radio, on to the technologies of today, has had similar effects, and there have been, I think, many revolutions in military affairs related to this shifting in the nature of information. No doubt we are in the middle of such a revolutionary period now.

In terms of the meeting that has brought us together here, to think about information and national security, we can surely agree that we are seeing a progression in the ability to diffuse information, to move it faster, to create that sense of immediacy that Peter Manning has addressed so very nicely in his paper. And with it, this tremendously increased interconnectivity, come some risks. That is, that the more that is known in the field, the more it is also known to the headquarters. This development may, in some ways, create an "attractive nuisance," encouraging a greater centralization of decision making authority.

A classic example of this phenomenon can be seen during the *Mayaguez* rescue mission 21 years ago, during which the President and Henry Kissinger were sitting in the White House Oval Office listening to what was happening as the Marines were going in on their helicopters. They could hear the bullets pinging off of the helicopters as they were descending toward Koh Tang island. And, at one point, Kissinger could bear it no longer, shouting gutturally from his chair: "Goh Leffft!" And so you can see, the urge to intrude from above is a very powerful one. That is one of the organizational or institutional risks that we have as we see information move forward through these new media that bring us ever closer to the front lines of what is happening--to events like the

real-time observation of the crash in the Everglades that Peter Manning has studied, and the organizational problems with response it highlights.

The most advanced view of information, as matter, gets a little spooky. I'm a political scientist, but let me talk a little physics for a few minutes anyway. Information increasingly has properties not unlike other physical things in the world, and the easiest way to think about it, at least for someone like myself, a bombs-and-bullets guy, is to think about weapons. Traditionally, weapons have been composed of a certain amount of mass, a certain amount of energy and, throughout most of history, not a lot of information.

In early times, with, say, the javelin, there is little "information content," limited to the intuitive calculations of the thrower, whose physical strength propels the device's weight, adding energy to its mass. Contrast this with the naval cannonball of the Age of Sail, where we have again a certain amount of mass, a certain energy, and a little more knowledge. Knowing when to fire on the ship's roll, firing in unison, sighting over a barrel, all these actions improved the information content a bit.

But what really has happened in the last 25 years is that we have seen a change of many orders of magnitude in the information content of weaponry. And that is while the mass and energy hurled by, say, a Tow missile, is perhaps not all that much dissimilar to the bazooka of the Second World War. The information content of these two is vastly different, though, as the Tow embodies a tremendous amount of information in addition to its mass and energy. Aerial bombardment has seen a similar effect take place. Look at the amount of ordnance that was needed to knock out a target in 1944, let's say a ball bearing plant; and then look to see how much ordnance was needed to knock out a specific target, like Iraqi intelligence Headquarters in 1993--in reprisal for the assassination plot against George Bush. What was needed in each case? In the former, carpet bombing--in the latter, one smart bomb.

So, we can see that the information content of weaponry has grown tremendously--the physicality of information emerging--and we are lucky to have some very insightful people, including Tom Rona and some of the scholars at the Air War College, notably George Stein, who are developing this new physics of information. Among their many ideas include notions suggesting that some bits of information attract others. That is, they have gravitational sorts of effects, they bring in other kinds of information, acting as what one might call "great attractors." My personal favorite--which I do not think they have bought off on yet, but I suggested they think about--is a black hole. In this context, it is, something sucking information in but never putting anything out. Should I be saying this here in Washington? I think I should move away from this topic--and right smartly at that.

Let us consider power for a moment. The ancient Persian empire was great because it was big. It was *really* big. It stretched from the Indus to the Aegean, and yet it was toppled over pretty easily by Alexander and his small army. He didn't have great

resources, but the resources he had were subject to organization in something called the phalanx, which the Persians just could not figure out how to fight. Two kinds of power are displayed here: the mass sort, the sheer quantity, and then the quality introduced by organization. And I'd say that, throughout history, we have seen a pattern of action and reaction between those who have viewed power quantitatively and those who have tried to refine it qualitatively.

This quality/quantity debate continues today, enriched further by the notion that power is increasingly becoming less intangible; a phenomenon that Joseph Nye refers to as "soft power," the kind one finds in ideas or beliefs, or belief systems. And I think no better example of this exists than in the 20th century success of so many guerrilla movements that did not necessarily espouse ideas about democracy and "feel-good" human rights, but which did have ideas about independence or autonomy or throwing off some colonial yoke. The idea of independence, which motivated our Founding Fathers 200-odd years ago, has motivated many small, weak peoples to stand up against far better armed, better organized overlords.

Throughout much of the 20th century, the materially weak have done quite, quite well. Lewis Gann has reported on this in his marvelous study, *Guerrillas in History,* which gives full credit to the importance of ideas. And I think we see this today with respect to notions of the attractiveness of democratic processes and market economics. Indeed, current American grand strategy is built around the idea of freedom, of free trade and free peoples. The ideas have a great deal of power to influence others.

One can look at the question of the dissolution of the Soviet Union and see the power of the idea at work there, too. Poland, for example, through the Solidarity movement, decided that it would no longer be a satellite--and soon it wasn't. Maybe President Ford anticipated the Poles in that 1976 debate gaffe of his, when he said that the Poles didn't consider themselves to be controlled by the Soviets. The power of their ideas of freedom sent a message to Moscow, and to all the outlying bastions of that dying empire.

We should talk now about how we are going to integrate these notions of information and power into national strategy. And it is important, I think, to look at strategy because, among other things, of these movements toward the materiality of information and the immateriality of power. We may find that we can transform states, and perhaps make them even more powerful than before. Some say we are seeing the end of the nation state. Some think we are at the end of history. Neither view is correct. History is re-awakening, and the state may actually be entering a golden age. For what we see in these developments regarding information and power, both diffusing, the one becoming more material and the other less so, may serve states better than any other form of political organization.

I mentioned empires earlier. What we are really seeing now is the death knell of the empire, the political unit that has governed international politics for the past 500

years, from Philip II of Spain, right on down to the Soviet Union. The 20th century, in particular, has seen a series of self-inflicted hammer blows of empire upon empire, with the last falling just 5 years ago. Well, maybe there is one left. Maybe the United States leads something of a benevolent empire of influence. But, we don't look like other empires--they are falling, with perhaps only this one left--and it is the nation-state that grows in numbers and power. There were 50-odd nations at the founding of the UN in 1945. Today, that number has trebled. The point is that there are a lot more nations. Nations and nationalism exist where there are states and where there are not. And so it is ever more important for us to think about questions of state power and the variegated effects of advances in information upon them.

How, then, can we begin to develop a "national information strategy?" In passing, let me note that I prefer this phrase to the term "information warfare." In many ways, the latter says both too little and too much. Because, as we have seen, information is a rich, multi-dimensional term, and warfare exists across a great spectrum. Also, I should think that here in Washington you would agree that information warfare as an organizing term or concept creates an immediate bureaucratic problem--which is that half of the U.S. government, the civil side, cannot deal with something that has "warfare" in its title.

If the military and civilian actors in government, and the private sector, are to interact with each other--which is the only way we will set a good information strategy--we have to realize that our paradigm must be one in which all can participate. Information strategy provides just such a "big tent." Information warfare doesn't. In some respects the current attachment to restrictive terminology goes to what Peter Manning was suggesting in his paper: that terms, or the arcana, of the information "business" are sometimes used as a means of setting up an exclusive "lodge" or club membership.

Is the professor just theorizing or are there examples of information strategy that are useful to think about? Let us take a very brief little excursion. Look at the Cold War and think of grand strategy in terms of the knitting together of political, economic and military capabilities and resources. The Cold War is almost a laboratory case of an open versus a closed system, a period during which the United States fostered, among other things, free markets, rife with as much information as possible to build up the world economy. The Soviets, on the other hand, took a far more proprietary, mercantilist, view of how things should be done, keeping close control over information, centrally planning, very proprietarily, their and their satellites' economies.

Politically, the U.S. put a great deal of effort into trying to spread its ideas around the world. The Soviet Union tried to keep ideas from its people and, of course, the price of the repression grew as information technologies advanced. Even the effort to spread to others their notions of the "workers' paradise" is best remembered as the dissemination of the "Big Lie."

In the military sphere, the United States had something of an open sort of view. We felt that openness and full information were the cornerstones of successful deterrence.

We felt that sharing of information was important to enabling the interoperability of systems which would allow coalitions to form and defend freedom around the world. Obviously there were proprietary areas where information was not shared, but a great deal was open. After all, in 1960, how many of you had the Revell Polaris submarine? I had one. And this was at a time when the Pentagon was horrified to see its finest weapons system on display in five-and-dime stores. A great deal of sophisticated information has always made its way outside of our system. And, in fact--on this other related point--you see in U.S. strategy an unswerving devotion to improving and expanding upon the information content in our military capabilities. This led to precision guided munitions, to all the smart weapons we see today, and the information systems that support them.

The Russians, on the other hand, stayed with that quantitative view of the basis of power. Stalin thought that artillery, as he said, was the God of War, was his Mars. And while some organizing was done to try to maximize Soviet society's output in the military sphere, there was, I think, a great deal of neglect of the informational side of the military components of national power. And what we saw at the end of this Cold War was that closedness could not compete against an open information strategy. *Perestroika* came along near the end, to try to open up the economy a bit, to reorganize, to share information. It happened too late. Politically the notion of trying to repress information was refuted by the rise of *glasnost*. Again, it came too late. All these things came a little late, a little short, and led to the dissolution of that closed-system empire.

Well, the question for us now is, if a good strategy worked when there was a tough opponent out there, will the strategy work even better when we don't have a mortal enemy, or at least we think we don't. And whatever view you want to take, whether it's a devil theory of Russia, or the transformed theory of the Russians, it's a system that is now less "track-based" than it used to be in terms of a focused, very dangerous adversary. Nevertheless, residual Russian power remains great, and should convince us of the need to continue to think strategically, to worry about capabilities even as we grow less concerned about intentions. For when we distrusted the Russians, we worried a great deal about capabilities that we now know were less powerful than we believed. Now, the challenge will be to avoid underestimating Russian capabilities in an emerging era of trust.

So should we continue with this openness? This is a question we have to engage, that you should be engaging in the national security areas, when we think about who should be doing sensitive work. Do we continue openness? We use information to enrich and enliven political, economic and military initiatives. I'm not sure as to our proper course. And in the chapter I mentioned previously--for those of you that would like to read that chapter that I wrote with my colleague--my co-author and I suggest that maybe what worked in the Cold War is not the best idea now. Maybe if we are entirely open and forthcoming with information about our political views and goals and objectives, others will calibrate their actions against us. Bosnia is a very good example--especially during the several years prior to the Dayton Accords--of the Serbs knowing exactly where we stood all the time. This enabled them to walk right up to the brink and to dance along it

during various crises for a couple of years. It was only when we became a little less clear, a little more willing to threaten credible, forcible options--and even to use some force, and I'm not sure how much more we would have been using--only when there was some doubt about possible U.S. actions did they come to the bargaining table.

It could be that in the post-Cold War we don't want to share political or diplomatic information freely with others. In the economic realm, it may not be that we want to share lots of information either. Prosperity and power in the future will relate a great deal to things like intellectual property and the warehousing of information. Information itself becomes a tremendous economic asset. It is not clear to me that what makes the classical market of Adam Smith work--free flows of information, wide sharing of information--will redound to our benefit in the information age. In fact, a more proprietary or guarded view of much of the centers of our commercial infrastructure may become necessary. Militarily, the same question comes up: Do we really want everybody to know about almost everything we have--as we did during the Cold War? I don't think so.

What we have now is not a single competitor aiming mortal threats at us, but a multiplicity of potential opponents who will attack our friends and interests in any number of places in the world. And the more they know about our precise capabilities, the more they will be able to tailor the threat to get around us. So, with openness, there may be a little bit of a problem. What about the problem of today's friends who may not be tomorrow's? Do we want to share full information with them? How much interoperability do you want to have with allies if the list of allies includes Syria? It could be that not all allies are "created equal," and that what one would share with Britain one might not with countries like Syria or with others--whose names, I'm sure, will come quite easily to mind.

The other side of this problem, of course, is that by not sharing one might encourage an "information arms race." And that could be a very nasty business as well. So again, a guarded strategy is what I would suggest, one that doesn't give away the new crown jewels but also doesn't encourage independent "breakouts" by other countries.

Lastly, on this issue of strategy I simply want to say that we need to think also of information as something that not only enriches or transforms the traditional political, economic and military dimensions in national power, but emerges as a separate form of power on its own. It doesn't always have to be used in conjunction with some other element in national power. Now let me give you an example of this. Think about Cuba. We have waged a 20th century version of the Thirty Years' War against Cuba. This war has included heaping helpings of military coercion, the attempt politically to isolate a regime and, of course, a rigorous economic embargo which only recently has been subjected to further tightening. None of these things work, I would suggest—in some respects partly because Castro's power is less derived from that first resource kind of power, or the second, organizational kind--and is based much more upon the third kind of power, which has to do with ideas. And his grand strategy is built around the idea of

Cuban sovereignty, that no one else will ever rule Cuba, that Cubans will rule it for themselves. Hugh Thomas's wonderful study of Cuba is subtitled, *The Quest for Sovereignty*--and this history begins in the 16th Century. This is a Cuban pattern that goes back hundreds of years. Hugh Thomas was quite sensitive to that idea-based form of power; and I think that Castro is very much steeped in that tradition of Cuban independence. He has tried to maintain his country's sovereignty. Well, what does this imply for us? Do we continue? Do we wage another Thirty Years' War against Cuba? Do we hope that if he dies or fades away that all will come apart. Or is it possible to think about using what one might call a fourth dimension of grand strategy--information as a separate arm of grand strategy. I think it's worth a try. Why don't we try to use information to reach out and touch the Cuban people directly?

In some respects, information today is a little bit like aerial bombardment from the 1930s--the rise of a long range bomber that can carry a pretty good payload. We're looking at an era (the 1930s) during which the notion of a homeland sanctuary was being lost--not unlike in the information age, when the idea that people can touch our systems anywhere, anytime, is gaining currency. Sanctuary was lost in the 1930s because the bomber could overfly your country whether your field armies had been defeated or not. And so today, in the information age, we may think of information as a way to reach another people without having to defeat their armies, without having to exhaust their economy. Cuba may be absolutely ripe for something like this. Simply passing the information to them about what the rest of the world looks like, how it operates, asking them "Wouldn't you like to join?" And if that were coupled with some kind of easing of either military or economic pressures on that country--sanctions which are presently, I think, actually being used by Castro to help maintain cohesion against an external threat--then I think we would see some very interesting things happening. Well, is it worth a try? I would say that 30-odd years of the one way not working suggest that we should give an information strategy a whirl.

In closing, let me just go back for a moment to Athena, Goddess of Wisdom, who sprang fully armed from the head of Zeus. That image is an important symbolic one for us. She was absolutely the fusion of information and power; and I think for the information age she may be a far better paradigm for us to think about and work with than old Mars. In fact, let me close by paraphrasing a popular current book title: "Cavemen are for Mars, the future is Athena's."

MICHELLE VAN CLEAVE

Ms. Van Cleave practices law in the areas of tele-communications, technology and industrial security, and is a frequent speaker and government consultant in these areas.

During the period 1987 through 1993, she held the positions of General Counsel and Assistant Director of National Security Affairs in the White House Office of Science and Technology Policy. During 1989 she served as Minority Counsel to the Committee on Science, Space, and Technology, U.S. House of Representatives.

From 1981 until July 1987, Ms. Van Cleave was Assistant for Defense and Foreign Policy to Congressman Jack Kemp, serving concurrently as national security assistant to the House Republican Conference and associate staff member, Appropriations Subcommittee on Foreign Operations.

Ms. Van Cleave is a member of the advisory boards for the National Security Academy of the National Intellectual Property Law Institute and the Center for Security Policy, and serves as a consultant to the CIA and Los Alamos National Laboratory.

MICHELLE VAN CLEAVE, Discussant, SESSION I

I have served as a discussant for a series of three presentations this morning which strike me as somewhat disparate in their texture and focus. I was struck by what Professor Manning said earlier, that people would look at a screen and try to come up with a Gestalt of what they are seeing. I'm not sure I've got a good Gestalt to present to you this morning about what we just heard. Perhaps the presentations will engender some lively discussion and allow an opportunity for a variety of issues to emerge. But if there is a common theme that comes out of these three presentations perhaps it is: What are the implications of the information revolution, particularly the national security threats posed by strategic information warfare, for the security disciplines including personnel security?

I'd like to offer some thoughts somewhat along those lines on and then open it up for all of the questions that I hope that you have been keeping track of as you heard these presentations today.

The world is in the midst of an information revolution that many believe will have as far- reaching an impact on politics, economics, and the culture as that of the industrial revolution. This phenomenon, even as it rearranges the fabric of modern life, will surely also affect the manner in which states and other international actors wage warfare. It will also affect the means by which they define and protect their interests, including their security policy and objectives. Overall, the explosion of information technology and the merger of communications and computers into information systems has brought tremendous benefits but, as this audience is painfully aware, ever more complex security concerns as well. As Secretary Paige points out, our ability to build networks has vastly outstripped our ability to protect them. And our way of life and very survival depend on information systems. They afford greater personal and commercial freedom. But, the national information infrastructure also presents lucrative targets.

Information warfare is defined by the Department of Defense as "actions taken to achieve information superiority in support of national military strategy by affecting adversary information and information systems while leveraging and defending our information systems." For DOD planning the offensive tools of information warfare have become integral to modern warfare as Desert Storm--dubbed the first IW war--revealed. The value of superior information is not a new insight for military strategists or for security practitioners. Indeed OPSEC managers, for example, are old hands at the defensive information warfare business. What is new is the order-of-magnitude changes in technology for manipulating information, as Secretary Paige has reminded us. Much creative energy--from R&D through attack operations--is going into the opportunities presented by offensive information warfare.

But the strategic dimension of defensive information warfare, or what's being called information assurance--protecting the lifeblood information systems of the nation--remains outside the scope of DOD activities. At the same time, the armed forces have an

increasing dependence on the domestic civilian infrastructure. While many of these systems are not traditionally considered vital to the conduct of military operations, they often play a vital role in mobilization and logistics. In the face of defense draw-down, consolidation, and force pull-back to the continental United States, DOD dependency on the US domestic infrastructure is at an all time post WWII high. As a result, adversaries may be able to appreciably undermine US military power by attacking information systems upon which the country depends.

An even greater concern is that adversaries could bypass an attack on US military power and attack the country directly through its information systems. Those systems, to an extent largely unknown, are vulnerable to attacks that may result in information compromise, loss, exploitation, manipulation, denial, destruction or disruption of the systems. And at the high end of this range of threats, there lurks the potential for a new form of strategic warfare, spanning the sort of things that many are calling information warfare.

Now, when it comes to the specifics of information warfare, there's a high level of unknown across three levels of concern: criminals, terrorists, and governments. The teenage kid hacking in his bedroom may not be a national security threat, although he or she could mess up your home computer or your credit record. Computer crime is a growing area of concern for law enforcement obviously, and overall no one knows the extent of the economic losses attributable to information attacks. But the potential for any economic loss, if not chaos,--is certainly there. Perhaps of more immediate concern to this audience is the potential for hackers to be in the service, witting or otherwise, of determined actors with a larger purpose.

For terrorists, physical destruction may be the method of choice, as we saw tragically in Oklahoma City and the World Trade Center. But the opportunity for a stand-off attack that would be untraceable, with an extremely low-risk of being identified much less being caught, makes information warfare very appealing from a terrorist's perspective. If you recall from the case of the World Trade Center, there was actually a higher dollar loss associated with loss of information disruption than from the physical destruction at the facility.

And finally, foreign governments. Here our intelligence is very spotty because there have been no prior intelligence collection requirements against this kind of offensive capability. In fact, there are difficulties associated with the intelligence community collecting such intelligence in that activities so frequently cross over into domestic targets where there are laws and precedents against IC monitoring. Presently, the first national intelligence estimate ever on the foreign threat to US information systems is being written. The largest contribution of this NIE, incidentally, is likely to be its usefulness in pointing out just how much we don't know.

What we do know best, though, are US capabilities in information warfare, and the more you know about the offense, as Secretary Paige discussed earlier today, the

more you are concerned about the need for protecting yourself. A strategic attack on the national information infrastructure would be a substantial attack on privately owned commercial network systems and facilities. Such an attack and its precursor elements might be first and only visible to industry owners and operators. The policy issues arising from this fact are very challenging: the constitutionality, legality, proprietary feasibility, nature and manner of how a government entity can perform or receive indications and warning information about such an act on the private infrastructure, and how threat data can be passed to industry and reliably disseminated for warning purposes.

And, unlike conventional warfare, the assessment of the who and where and why of an infrastructure attack may be extremely difficult. The technical dimensions of information warfare techniques are likely to obscure what in most other cases would be obvious (i.e., that country X was attacking us.). Therefore, attack assessment for infrastructure assurance may require extensive (and intrusive) "active" electronic operations, rather than "passive" monitoring. Chasing an IW attack back through the information infrastructure to the attacker's origin not only may be technically difficult, but immediately runs up against a number of legal prescriptions. It is likely that only the most sophisticated IW activities themselves would have the technical capability to perform this function but may be legally constrained from taking action.

Indeed, the advantage in information warfare in the future is likely to remain sharply with the offense. It may turn out that the only way for the United States to mount a fully credible information infrastructure defense is to develop a mechanism by which offensive skills and capabilities can be used to aid its defensive needs, while at the same time protecting the essential secrets and the security of its offensive capabilities. A serious effort by national security planners to design and implement a mechanism for deriving this benefit from the offense may need to be the highest priority for national information assurance strategy. In fact, it seems to me that the development costs of such an effort may turn out to be a fraction of what the US stands to lose if it is unable to develop a comprehensive information assurance program.

Finally, information assurance will depend in large measure on the degree of our preparedness to withstand an attack, which may well include, of course, security, countermeasures, hardening, emergency back up capabilities, design resilience and flexibility, O&M stock-piles, self-reliance plans and programs, and reconstitution capabilities. What is needed at a national level for our various strategic systems, therefore, is risk assessment, and risk management, at the strategic level for these vital information systems that make up our infrastructure. And that will require a government/industry partnership of unprecedented scope. At present, there is no national strategy or policy for information assurance. Yet, many activities are under way that contribute to national preparedness against information attack. For the most part, these are not undertaken for the purpose of information assurance, but for other reasons. The private sector conducts such things as planning against national disasters, or assuring the confidentiality and availability of computer records, and protecting the privacy of communication on the reliability of financial transactions. Industry's standard for liability

and insurance purposes may also contribute to an overall national preparedness for information assurance.

Many government disciplines and missions also contribute to this mix, including virtually all of the security disciplines represented here today as well as disaster response teams, counterintelligence officers and national security planners. For the most part, these various communities have little interaction and virtually no awareness of how they might interrelate against the background of this national requirement. The disparate activities that contribute to Information Assurance can be pulled together into an overall national information assurance strategy, but, that will require leadership. Some of that is slowly beginning to emerge, as some of our speakers at this conference suggest.

I also believe that this education effort will require a serious public policy debate, not just narrowly focused interest-group politics, but a serious public debate about the place of, an information security policy in American society. In this regard, I was struck by John Arquilla's admonition that we need to find ways to protect our nation's strategic information and information systems in both government and that private sector that also support our values and our deeply held belief in, and respect for, individual rights. And I'm confident that this can be done. Americans believe in a free marketplace of ideas, but we also believe in privacy and in property rights. The protection of those things we hold dear is equally the province of our cherished democracy as is their advocacy. In this regard, Professor Manning's presentation on loyalty inspires me to close on a different note.

I had occasion recently, because I was driving off to see a friend over the weekend, to precede for about a 30-mile stretch the Olympic torch that was being carried out from Washington. And it was fascinating to me because I was driving along in these back streets in Virginia, on a day when it was a 100 degrees in the shade and the humidity was just horrible. And there were people lined up both sides of the street--everywhere you could see--with their American flags and their hats and balloons. And they were excited and they were having a great time and they were waiting for the Olympic torch to come by. And this outpouring of identity and of spirit and of patriotism is striking to me truly as an American phenomenon. I don't know that that kind of spontaneous expression of patriotism and support for country is that common in other countries. And it made me smile, and it was a wonderful thing. But even in our land of widespread patriotism we have spies.

It remains unclear why. Certainly in the Cold War, millions of people had access to national security information and only a tiny handful engaged in espionage. Of course, a sizable chunk of those were not in it for the money. Rather, their motives were either ideological or antisocial. Professor Manning's discussion of the impact of information technologies on organizational loyalties suggests that the situation now may be worse than it was during the Cold War, further exacerbated by the fact that the patriotic impetus working against treason and disloyalty is not as clear today. You could be selling out your company or your office or your boss, providing that inside information, without

realizing that you're also selling out your country. And there has been an apparent lessening of civic virtue among some, which does not bode well for personnel security. So it would be a mistake to think that information warfare questions are just technical issues. Like everything else, it is human beings who are at issue here. Yes, there are technical attacks facilitated by the tools of information technologies. But humans are still the source of trouble. Ted Sarbin set the theme for this conference around that point. Technical solutions alone will not suffice. We need to look at individuals and there the answer must turn back to education and understanding in the information realm that hacking and these kinds of intrusions that go on all the time in the anarchic environment that constitutes the information realm are really in fact crimes. That they are wrong, that they are immoral. We, in sum, need to extend some sense of civic virtue and personal responsibility into activities over the Internet. Real damage can be done by those who are just out to have a good time. And people need to understand that. It may be that high schools, for instance, and secondary schools and others that are turning to computers because of what they bring in value as an instructional tool also need to be teaching students morality in computer usage. What is right and wrong in that world.

For security practitioners, security isn't about coming up with a bunch of rules. It isn't some gum shoe-like undertaking to be exploited by political operatives looking for advantage over their political opponents. It's also not some undertaking to be exploited by the professionals. Professionals can't just go around putting people on report. Security itself is a moral issue, like respect for the law and for the rights of others. You can't write enough laws and regulations to stop crime. You have to instill a positive attitude about personal responsibility, law and justice. The same is true with security. Individual responsibility to protect security measures because they support what we as a nation value most is needed from the most junior clerk to the commander in chief. It shouldn't be that we leave civic virtue back in the 18th century as we move into the information age. For security professionals that means approaching our jobs always in conformance with our values for the purpose of protecting our liberties.

But first we need the respect and confidence of the American people. Among other things, I am a lawyer. I am concerned about the reputation of my profession and the proliferation of lawyer jokes that suggests that there is some reason to be concerned. I think that the legal profession has difficulty with many people who believe that lawyers misuse the law to serve other purposes, other than the high calling of fairness and justice. I'm concerned in many respects that the same attitude may pertain to people's views of security officers. The tools that we use as security professionals--and for reasons in my past I count myself among you--are very powerful. Loyal Americans rightly fear the misuse of background investigations, polygraphs and such--things which affect reputation are viewed, rightly so, as very powerful. We must exercise care not only that we not misuse them, but that in the same way we not *appear* to misuse them. The appearance of misuse has the same effect as misuse because it scares people. In this regard, reports of White House personnel officials abusing access to FBI files are especially damaging, whatever the truth behind their actions. We all know among our acquaintances people who are perfectly loyal and careful protectors of our secrets who, nevertheless, have a

fear of people poking around in their most private thoughts and in that private person that we don't normally show to the world.

The unethical misuse of this system combines with this perception to cause fear of potential unfairness and arbitrariness, disdain for the regulatory burden and the system that seems like a Customs Service of a third world despotism or that makes the Department of Motor Vehicles seem user friendly, and a sad exasperation that, when all is said and done, the system still didn't prevent the decade-and-a-half of the spy. Because there is validity behind the fears and disdain and exasperation, the bureaucrat and political opponents (within and outside the government) who oppose counterintelligence and security and countermeasures for other reasons can use this as leverage to stop needed reforms.

The American value of privacy is precious and when we have to make intrusions upon it in the name of security, we in the security business carry tremendous responsibility to demonstrate that our efforts are fair, consistent, and reasonably related to our ends. It is incumbent upon us to show that, both because it is right and to preserve our values, and also because a perception of unfairness damages the fabric of trust that is the ultimate reservoir of security that really keeps our secrets.

SESSION II

ERIC BIEL

Mr. Biel is presently Staff Director of the Commission on Protecting and Reducing Government Secrecy, chaired by Senator Daniel Patrick Moynihan. He is responsible for coordinating all activities of the 15-person staff of the 2-year bipartison Commission, which was established by Congress in 1994 to study and make recommendations concerning classification and declassification of national security information, personnel security, information systems security, and other related issues.

From 1990 until 1995, Mr. Biel was the Trade Counsel with the U.S. Senate Committee on Finance, advising the Committee and formulating legislative proposals for the Chairman's consideration on a wide range of international trade matters, including the Uruguay Round agreements, NAFTA, U.S.-Japan trade relations, European market integration process, U.S.-Canada trade relations, and linkages of trade to environmental, labor rights, and foreign aid policies.

Before joining the Senate Committee on Finance, he worked as an attorney in private practice in Washington, DC, specializing in international trade/transactions, immigration, and human rights.

REMARKS ON BEHALF OF SENATOR DANIEL PATRICK MOYNIHAN, CHAIRMAN, COMMISSION ON PROTECTING AND REDUCING GOVERNMENT SECRECY

Eric Biel

Thank you for the kind invitation to speak this afternoon. In particular, let me thank Ted Sarbin and Roger Denk of PERSEREC. The Commission staff has benefited greatly from working with the two of them and their colleagues in Monterey over the past several months.

I obviously am not Senator Moynihan, but I will attempt this afternoon to offer some thoughts on his behalf. And I have given Scott Armstrong--in his role as discussant--a copy of the reissued version of Edward Shils' classic 1956 work, *The Torment of Secrecy: The Background and Consequences of American Security Policies*--with a new Introduction by the Senator.

In fact, let me stress that I view my purpose here today as to speak on behalf of the Senator. This is *his* perspective--not that of the Commission on Protecting and Reducing Government Secrecy as a whole. In fact, we still do not know what our 12 Commissioners will have to say on the variety of classification, declassification, personnel security, and information systems security issues that we--and many of you here today--are struggling with.

With that in mind, I do not intend to focus my remarks today on the ongoing work of the Commission. But I certainly would be pleased to answer any questions you may have about us--our organization, objectives, timetable, and so on, and what "protecting and reducing secrecy" is meant to convey.

Revelations during the past year have quieted much of the remaining academic debate concerning the nature of the security threat that confronted the United States during the mid and late 1940s. *The Secret World of American Communism*, published last spring--Harvey Klehr and John Earl Haynes' masterful analysis of documents obtained from recently-opened state archives in Moscow--clarified a great deal concerning the secret Communist activities in this country during the later stages of World War Two and in its immediate aftermath. The releases over the past 11months by the NSA of the so-called VENONA intercepts--there have been three to date, with a fourth expected within the next few weeks and the remainder of the 2200 intercepts due to be released by the end of the year--have confirmed considerably more about the scope of the Soviet atomic espionage ring and other Communist spying here. About already well-known figures such as Klaus Fuchs, Julius and Ethel Rosenberg, and Alger Hiss. With important revelations as well about heretofore little-known persons such as Theodore Alvin Hall, code-named "Mlad," a 19-year old Harvard undergraduate and member of the Young Communist League, the VENONA intercepts tell us, and perhaps along with Fuchs the key spy at Los

Alamos. The intercepts also tell us of activities the very existence of which had been matters of intense and hostile debate only a short time before.

Senator Moynihan regularly notes how pleased he was to play a part in the initial VENONA release at the Central Intelligence Agency on July 11, 1995. From those 49 documents concerning atomic espionage directed against the Manhattan Project we learned that, within half a year of Army Signals Intelligence officer Meredith Gardner's first "breaking the code" on December 20, 1946, at least some within the U.S. Government understood well the nature and magnitude of the espionage threat.

And by 1948, the Soviets would know that we knew what they were doing: an American cipher clerk named William Weisband passed the information on, though he was not discovered until 1950 (and never prosecuted due to abiding concerns about revealing "sources and methods" in a judicial proceeding). And Kim Philby, working as an intelligence liaison officer at the British Mission in Washington, began receiving summaries of VENONA translations in 1949; shortly thereafter, the K.G.B. changed its codes.

But it took nearly half a century for the Government to tell the American public what it knew about the Communist efforts to steal THE SECRET. As well as other aspects of Soviet espionage activities gradually and painstakingly uncovered by Mr. Gardner and his colleagues at Army Signals Intelligence.

And, at least as importantly, it took quite some time to share the information about Soviet espionage--and the involvement of Americans in it--*within* the Government. Some, including in all likelihood Dean Acheson and perhaps Harry Truman as well, never were so informed.

Now to appreciate why this matters so deeply to Senator Moynihan, one has to understand that he "came of age" in an academic and political sense--after serving in the Navy at the tail end of World War Two--in New York City in the late 1940s and early 1950s. Where, apparently, everything you needed to know about a person centered around his or her views on whether Alger Hiss was guilty of espionage (although, of course, he never actually was tried for espionage, only for perjury).

All of which caused Senator Moynihan to set out some thoughts on the subject of VENONA in *The Washington Post* 10 days after the initial July 11 release--in a short piece titled, "The Price of Secrecy."

Allow me to quote from its concluding paragraphs, in which the Senator explained what he saw as the chief consequences of the Government's decision not to divulge the truth sooner:

In 1956, Edward A. Shils of the University of Chicago published *The Torment of Secrecy: The Background and Consequences of American Security Policy.* He captures just the mood of the early 1950s:

The American visage began to cloud over. Secrets were to become our chief reliance just when it was becoming more and more evident that the Soviet Union had long maintained an active apparatus for espionage in the United States. For a country which had never previously thought of itself as an object of systematic espionage by foreign powers, it was unsettling.

The larger society was facing "an unprecedented threat to its continuance." In the circumstances, "The fantasies of apocalyptic visionaries . . . claimed the respectability of being a reasonable interpretation of the real situation." A culture of secrecy took hold within American government, whilst a hugely divisive debate raged in the Congress and the press.

Some saw conspiracy everywhere. Recall that in 1951 Sen. Joseph McCarthy published "America's Retreat from Victory: The Story of George Catlett Marshall." Some denied any such possibility and accused the accusers. Loyalty oaths and background checks proliferated, and all information became Top Secret. As the scientists could have told us, this deeply impaired our analytic capability, even as it concealed the decline.

We got through it. But the world remains a dangerous place, and it is just possible we might learn something from the VENONA files. Had they been published in 1950, we might have been spared the soft-on-communism charge that distorted our politics for four decades. We might have been spared the anti-anticommunist stance that was no less unhelpful. We might have been spared the execution of the Rosenbergs.

What if we had? In any event, what if a not dissimiliar crisis arises in the future? What if this time we opt for openness?

The Government could not do so then. Thus, we "learned" of the Communist conspiracy not from the Executive Branch of our Government but primarily from a demagogic Senator from Wisconsin and his aides. With all of the awful consequences that followed for personal reputations and careers and for the legitimacy of government institutions.

Let us fast-forward nearly half a century. Senator Moynihan is acutely aware of the dramatic changes that have taken place in security policy over the past few years through the efforts of the Joint Security Commission, Security Policy Board, PERSEREC, Information Security Oversight Office, and others, and the leadership of senior policymakers--including John Deutch, a member of our Commission. Executive Orders 12958 on classification policy and 12968 on personnel security matters, as well as the National Industrial Security Program developed pursuant to Executive Order 12829,

all demonstrate elements of "new thinking" about different security issues. Together, they form the backdrop for this conference on "Security Issues for the Next Quarter Century."

But from another perspective, it remains legitimate to ask how much really *has* changed in the intervening four decades since Shils wrote *The Torment of Secrecy?* Are important elements of the classification and personnel security systems still grounded on principles with which Shils would have been quite familiar?

Where are we today? According to the Information Security Oversight Office, responsible for counting such things, in 1994 there were nearly 4.8 million new Government "classification decisions"--down a bit from previous years, but at the same time most certainly an underestimation of the actual number. (We will learn about 1995 figures very shortly when the ISOO issues its next report.) According to the General Accounting Office, in 1993 there are nearly 3.2 million persons holding security clearances--2,368,000 Government employees, another 853,000 working for industrial contractors. Figures which, the GAO notes, do not include CIA employees or contractors, nor those granted clearances for access to "Sensitive Compartmented Information."

John Carlin, who had just been confirmed as Archivist of the United States when he appeared before our Commission last June, estimates that the National Archives has roughly *half a billion* pages of information awaiting declassification, a number which excludes those documents still held by individual agencies rather than the Archives.

It is true that these numbers should be interpreted with great care. At the same time, it does seem reasonable to suggest that the costs of secrecy--both those that we *can* quantify and the untold consequences for democracy, the level of public trust in government, and so forth--are staggering.

As has been reported widely in the media in the past day or two, the latest estimate of the costs of "classification-related security measures" to the Federal Government--the result of an impressive product developed by the SPB's Security Costs Working Group and officials from ISOO and OMB--is approximately $2.7 billion for each of FY 1995 and 1996. And, while that does include the NFIP account at DoD, it does not include CIA figures, which were provided through OMB to the Intelligence Committees in classified form only.

The costs to industry, most of which in turn is passed on to the government and thus the taxpayer, have varied widely in different surveys. The latest extrapolation appears to place these in the range of $3 billion to $4.3 billion, lower than earlier estimates, to be sure, but certainly not insubstantial.

And these efforts to estimate costs through traditional accounting techniques most likely only scratch the surface. For they cannot possibly measure what economists would term the "transaction costs" associated with secrecy, such as the expenditures needed

when officials of one agency must struggle to gain access to documents classified by another, or when those from one agency assert their "equities" to hold up release of materials stored elsewhere.

Nor the "opportunity costs" that arise when, for example, the security clearance process keeps talented individuals away from government service. These are the vast "hidden costs" lying below the surface in the clever "cost iceberg" diagram developed by the Joint Security Commission in 1994.

Aside from the costs already mentioned, the classification of large amounts of information that should not be classified can erode the entire system's credibility. As Justice Potter Stewart stated (in a quote that somehow has not received the attention given his famous comment on pornography): "When everything is secret, nothing is secret." Or, at a minimum, nothing remains secret for very long when there is disdain for the overall system.

Excessive secrecy in turn can contribute to a potentially dangerous mentality that dismisses "leaks" as harmless--simply one part of "normal" policymaking. It can lead to information being viewed as "*only* CONFIDENTIAL" or "*only* SECRET." It can lead to a proliferation of compartmented Special Access Programs--with all of their additional costs and security measures--that are created because the so-called "regular" (collateral) classification system is viewed as unable to provide the necessary safeguards for certain projects.

Which is not to say that these and other matters relating to the secrecy system simply have been ignored over the years.

Allow me to quote from one study examining the problem of excessive government secrecy:

> ...overclassification has reached serious proportions...the system has become so overloaded that proper protection of information which should be protected has suffered...the mass of classified papers has inevitably resulted in a casual attitude toward classified information, at least on the part of many.

Mind you, that was not the Joint Security Commission in its March 1994 *Redefining Security* report to the Secretary of Defense and Director of Central Intelligence. It comes from *1956*--in one of the first reports on the then-still young postwar classification system. (The same year, notably, that Shils' *The Torment of Secrecy* was published.) And, it may surprise you to learn, those words were written by a Defense Department committee (the Coolidge Committee) charged by then-Secretary of Defense Wilson with investigating *leaks*. Perhaps they simply could have cited Benjamin Franklin: "Three may keep a secret if two of them are dead."

All these years later, and notwithstanding the considerable efforts devoted to moving from risk avoidance to a more thoughtful risk management approach to classification management, we still would appear to have what one might call classification by autopilot--whereby classification decisions are often made without much thought to the consequences and long-term costs. For example, several times our Commission staff has asked their government briefers why certain briefing slides were classified--only to be told by the very people who prepared and classified those slides that they *did not know why*, but it always had been done that way!

In short, despite the best efforts of various commissions and task forces, despite a series of Executive Orders--most recently, the two new Orders signed last year--the most serious problems persist. In fact, in this Information Age, the problems actually proliferate--as the pace of creating, disseminating, and copying documents increases rapidly, and as the difficulties of protecting information being communicated electronically rather than on paper also continue to mount.

Senator Moynihan certainly has no illusions concerning the task at hand. Limiting unnecessary classification--changing the "casual attitude" cited in the report to Defense Secretary Wilson way back in 1956--will not be easy. For at its core, in his view, government secrecy is simply another mode of regulation, nothing that the great students of bureaucracy--from Max Weber to James Q. Wilson--would find terribly unusual in its operation.

Viewed as such, it should not be surprising that the Government has had a great deal of difficulty even contemplating the concept of deregulating *itself*. Even the new Executive Order signed into law by President Clinton last April, while making significant changes to the 1982 Reagan Order with respect to declassification of older historical documents, is fairly timid when it comes to the day-to-day workings of the secrecy system. And the first few months of the new Order's implementation have not been terribly promising from the perspective of those hoping for greater openness.

In part, this has been due to resistance by some officials to implement the Order's more important provisions and, in part, from the lack of an ability and a commitment to devote the resources needed to implement the Order.

It helps to have some pressure for change coming from the outside as well. Thus, our Commission. We are only the second *statutorily based* commission asked to study this subject of which I am aware, coming 40 years after the first, the Commission on Government Security, chaired by Lloyd Wright. (We hope to do a bit better than the Wright Commission, which ran into considerable controversy over a particular recommendation that was viewed as inhibiting press freedoms. And we hope to produce something a bit shorter than the Wright Commission's 807-page final report!)

We have a clear statutory mandate, contained in the Foreign Relations Authorization Act for FY 1994 and 1995 (Public Law 102-236), to "make comprehensive proposals for reform" that will "reduce the volume of classified information." Our Commission is examining whether by reducing the amount of classified information generated at the outset, we can reduce the other related expenditures--including the personnel and physical security costs I mentioned--and, in this era of smaller government, better use our limited resources to protect those government secrets that truly are sensitive, and the systems that carry them. Thus, our title: the Commission on *Protecting and Reducing* Government Secrecy.

Adopting a start-from-scratch approach, our Commission intends to reexamine the basic underpinnings of the classification and personnel security systems. Security systems that, despite periodic tinkering, still remain grounded on principles seen as suitable to another very different period.

You need not take my word for it. Not long ago, during the course of briefings for the Commissioners, a personnel security specialist made a most cogent observation. Noting that the system for clearing government employees still is governed primarily by rules established 45 years ago, he acknowledged that personnel security officials often are viewed by their colleagues as "dinosaurs . . . vestiges of McCarthyism"--perceived correctly as being stuck trying to apply standards developed in the early 1950s--and still enshrined in Executive Order 10450--to ensure primarily that the Government was free of individuals whose loyalty was questionable on ideological grounds.

We will be issuing our final report in early 1997--about one year from now--to both the 105th Congress and the President. Not knowing, of course, exactly who our ultimate audience will be, a circumstance that should remove any doubts about our bipartisanship.

One of Senator Moynihan's chief objectives with respect to our Commission is that those responsible for the day-to-day conduct and administration of classification, personnel security, and related security matters simply will pause to give serious thought to how they can best approach their responsibilities in this post-Cold War era. And to the consequences of a system that has the potential to severely limit citizens' understanding of their own history and the operations of their government.

Several weeks ago, Senator Moynihan and several other Commissioners spent a morning being briefed by two senior intelligence officials on some of the more arcane issues associated with the protection of sources and methods. In the context of an interesting discussion on how to balance secrecy and openness, to ensure both that

necessary information is disseminated to policymakers and sources and methods are protected, one of the officials noted that he had learned a simple lesson from his 33 years' experience in government: "If you want secrets to be respected, make the secrets respectable."

Toward that end, I can say on behalf of the Senator that the Commission welcomes the opportunity to work with all of you in developing new approaches for a security system that is tailored to the beginning of the 21st century--and has a "Vision 2021"--rather than the middle of the 20th.

STEVEN AFTERGOOD

Mr. Aftergood is a senior research analyst with the Federation of American Scientists in Washington, DC, where he directs the Project on Government Secrecy. Since 1991, he has edited the Federation's Secrecy and Government Bulletin, a monthly newsletter on national security classification policy and related issues.

Since joining the Federation of American Scientists in 1989, Mr. Aftergood has conducted studies in a number of areas in the fields of energy, environment, space policy, and government information policy. These have covered such subjects as space nuclear power, atmospheric effects of launch vehicles, and government secrecy.

The Federation of American Scientists, founded in 1945 by Manhattan Project scientists, is a national organization of scientists and engineers concerned with issues of science and national security policy.

THE NEED FOR SECRECY REFORM

Steven Aftergood

As a nongovernmental consumer of government information, I am naturally more concerned about issues of access and openness than about security. But I have quickly discovered that the two are linked together. Reducing the scope of the secrecy system will almost automatically improve the quality of security, even without a lot of other necessary changes. But without reducing the scope of secrecy, then most other efforts to improve security may be pointless and futile.

Anyway, I want to discuss some perceptions of national security information policy from outside the system, and talk about what it all may mean for security policy in the future.

To begin with, I would distinguish among three types of secrecy.

The first is genuine national security secrecy. This pertains to that body of information which, if disclosed, really could damage national security. And of course, I do acknowledge that there are many such secrets--I don't know anyone who doesn't. They include things like design details for weapons of mass destruction and other advanced military technologies, certain types of diplomatic and intelligence information, and so on. This kind of information is the reason we have a secrecy system in the first place, and when it is working properly this system positively serves the public interest.

The second category is what could be called bureaucratic secrecy. This has to do with the tendency of all organizations to control the information that they release to outsiders, including other government agencies. Bureaucratic secrecy explains, for example, why the White House never told Congress, even on a classified basis, that it knew that Iran was shipping arms to Bosnian Muslims. The inertia created by bureaucratic secrecy also helps account for the fact that there are billions of pages of documents that are decades old that remain classified even though, in the majority of the cases, their sensitivity has long since lapsed.

The third category is political secrecy, which refers to the deliberate and conscious abuse of classification authority for political advantage, irrespective of any threat to the national security. This is the smallest of the three categories but it is also the most dangerous to the political health of the nation. Maybe the most extreme example of political secrecy is the classification of radiation experiments on unknowing human subjects. But this category also includes more petty abuses like the classification of the size of the intelligence budget, which is done to protect the turf of congressional oversight committees, not the security of Americans.

This mixture of legitimate secrecy, bureaucratic inertia, and self-serving abuse of classification authority has been with us in more or less its present form for nearly 50 years. But I think it is reaching a crisis point whose outcome will help determine the security policies of the early 21st century. This crisis is manifest in several different ways:

1. Unauthorized disclosures ("leaks") of classified information are on the rise.

Secrecy has been applied so indiscriminately, and the system has become so bloated with classified documents that are not really sensitive, that the secrecy system is suffering from a kind of "inflation," like a Third World country that keeps printing more and more currency to prop up its economy. In fact, government statistics suggest that perhaps one out of every three pages of currently classified documents should not be classified at all, even by the government's own criteria. The result is that the value and significance of national security classification has been seriously eroded and unauthorized disclosures of classified information have become increasingly commonplace.

I used to clip and file every newspaper article that quoted from a classified document--lately there has been a flood of such articles in the *Washington Times*, for example--but it just got to be too much, and now I only save the articles that are of particular interest to me.

I don't want to exaggerate this claim--probably 99.9% of all classified documents remain securely in official hands and vaults, and the government successfully keeps lots and lots of secrets. But even so, leaks are on the rise and they are affecting, or even distorting, the way government does its job.

For example, it has been reliably reported that the White House rejected the idea of asking the CIA to engage in covert action in Bosnia, because the Administration was convinced that it would inevitably leak. I am not a big fan of covert action, but the point here is that a perfectly legal policy option was foreclosed in advance because the classification system could not be relied upon, and that's a remarkable fact.

In a study for the Department of Energy, Arvin Quist estimated that an average of one in 100,000 cleared personnel is a spy, based on the historical record, but that the number of leakers may be as high as one in 1,000. I don't think I know 1,000 cleared people, but I have received unauthorized disclosures of classified information from a lot more than 1 individual.

In fact, my own active interest in secrecy policy began in 1991 when I received an unsolicited stack of classified documents from an unacknowledged special access program called Timber Wind, an SDIO program to develop a nuclear reactor-driven rocket engine. Over the years, I have received classified material of almost every variety, from special access to restricted data.

It has gotten to the point that my organization has had to adopt a policy for handling classified documents! Our position is that even if the government practices indiscriminate secrecy, that does not mean that we should practice indiscriminate openness. And so I am not supposed to unilaterally publish classified information in my newsletter without going through our organizational procedures.

This is a responsibility that we take seriously--we don't even release unclassified information if we think that it would undermine national security. But the fact that we are in the position of having to decide whether classified information should or should not be made public is a sign that the system is sick. It is breaking down around the edges and down the middle.

On the other hand, until the secrecy system can be brought under control, I think leaks are necessary and often desirable because in many cases, they offer the public the only way to monitor crucial government activities.

2. Secrecy policy rewards ignorance.

Of course, the government also declassifies millions of pages of documents every year. But recent declassification policy has problems of its own. To an alarming extent, declassification policy rewards public ignorance and encourages conspiracy theories.

For a citizen to simply ask for a document that may be classified (even though it is not sensitive) usually doesn't work. Or else it takes months or years to get a response. So what does work?

Well, if you believe the CIA helped kill President Kennedy and you can persuade enough people that you may be right, like Oliver Stone did, you can get a wonderful law passed like the JFK Assassination Records Act. That law has led to an extraordinarily diligent declassification program leading to the release of many hundreds of thousands of pages. Of course, almost all of those pages should have been declassified years ago, but it took Oliver Stone to actually make it happen. That is disgraceful, in my opinion, and it sends a terrible message about what it takes to compel responsible government behavior.

Similarly, if you believe that an extraterrestrial space ship crashed in New Mexico in 1947 and the government conspired to cover it up, you get an impressive declassification effort together with a dedicated investigation by the Air Force that conducted notarized interviews with surviving military officials from that period.

If you believe the government covered up information about surviving POW/MIAs that were deliberately abandoned in Korea and Vietnam, you can also motivate a reasonably thorough investigation.

Unfortunately, the message that comes through in all of these cases is that the most effective way to get information declassified by the government is to engage in conspiracy mongering, and the more outrageous the better. But ironically, once the conspiracy theory that is needed for declassification has taken hold, all the declassification in the world is usually insufficient to uproot the conspiracy from the public mind.

In this way, current classification policy promotes public ignorance and degrades American political discourse.

3. Secrecy policy promotes an adversary culture.

Even among people who are not prone to conspiracy theories, secrecy tends to promote what may be called "the adversary culture." What I mean by that is a social and political climate in which the government is viewed as an adversary and in which the classification system in particular is viewed not as a means of protecting the nation and serving the public, but as a tool for deceiving the public and blocking government accountability.

There is at least some objective justification for this perception. Classification has certainly been used at times as a shield not against foreign enemies but against the American public. One of the most clearcut examples of this practice is presented in a 1947 Atomic Energy Commission memo on human experimentation programs which states that:

> It is desired that no document be released which refers to experiments with humans and might have adverse effect on public opinion or result in legal suits. Documents covering such work should be classified "secret."

This particular policy apparently ended in the late 1940s or early 1950s but some people believe it represents a continuing tendency in classification to suppress controversial activities. Or at a minimum, many people believe that there is no effective barrier in place that would prevent classification from being exploited in this way.

Who are these people? That's an important question. Before we invest lots and lots of time and money and resources in changing secrecy policies, we ought to find out, who really cares? Is it just a bunch of self-proclaimed public interest busybodies? Environmental extremists? Disarmament zealots?

The fact is that a majority of the American public believes that the government keeps too many secrets. That's what the Department of Defense found last year in a public survey commissioned by PERSEREC, the sponsor of this conference.

Specifically, in response to the following assertion:

"Given the world situation, the government protects too many documents by classifying them as SECRET and TOP SECRET"

DOD received the following response:

Strongly agree	13.9%
Agree	42.0
Neither agree nor disagree	17.1
Disagree	17.5
Strongly disagree	4.4
Don't Know	5.0

This is an extremely important finding in my opinion, because it shows that openness is not simply a special interest issue--it's the will of the people.

And for many people secrecy is not just an abstract issue. It is true that most Americans are not consumed with a desire to learn more about the history of the Cold War, and most people don't even care about efficient government or upholding democratic principles.

But they do care intensely about their health and the health of their families, about the safety of their environment and other immediate personal issues, where their interests are at odds with classification policy.

Recently I got a call from a woman whose father was listed as missing in action in the Korean war. She said that in response to a FOIA request, the National Security Agency had identified a document with her father's name in it but told her that she could not have the document because of national security reasons. Now she could not imagine any national security reason that was more important than learning about her father's fate, particularly when it involved records that were more than 40 years old. She was in tears and she was furious. She was convinced that the classification system is the enemy of her family and she was ready to do anything she could to circumvent it. If there were a black market for buying stolen classified documents, she would have been lining up to buy the documents she wanted.

Now if you multiply her case by the many thousands of people who have been affected in some deeply personal way by government secrecy--whether it's people who believe they have been injured by environmental contamination at government nuclear facilities or human radiation experiments or domestic counterintelligence activities or whatever--then you can begin to understand some of the passion that drives public opposition to government secrecy.

Certainly most of this opposition is expressed through legal channels. But it feeds a widespread contempt for the classification system that is gradually eroding classification's authority and effectiveness.

There are numerous other manifestations of the adversary culture.

One entrepreneurial fellow is selling T-shirts bearing an encryption algorithm that the Clinton administration considers a munition whose export is prohibited under the export administration laws. An advertisement for this product appeared on the Internet recently:

> Now you can wear a T-shirt that has been classified as a munition by the US government. That's right! The US International Traffic in Arms Regulation (ITAR) makes exporting cryptographic materials illegal....
>
> ...if you wear the munitions T-shirt where a non-US/Canadian citizen can see it, even if it is inside the US, you have just exported cryptographic material (which is already freely available outside the US) and have become a criminal in the eyes of the US Government.
>
> Now you too can become an international arms dealer for the price of a T-shirt ($15.95 to $29.95, depending on size).
>
> ...If you get arrested for wearing the Munitions T-shirt, we'll refund your purchase price...

Depending on your point of view, this is either a clever form of civil disobedience, or a juvenile prank, or something worse. But what is significant, I think, is that it displays a lack of respect and in fact a sense of defiance towards government authority, and towards information security policies in particular.

At any rate, it is clear that there is a problem with the national security classification system, and the problem is increasingly recognized inside and outside of government.

The good news is that under Executive Order 12958, policy is changing. For the first time in perhaps 20 years, government statistics will show that the secrecy tide is turning: More documents were declassified in 1995 than were classified. The difference in 1996 will be even more stark: The National Archives alone has declassified more than 60 million pages in this fiscal year with several months left to go.

The new policy has put a lot of strain on classification officials, and they have a really tough job. It is even tougher because no one is going to say thank you to those officials if they do their job right, but lots of people--like me--are going to criticize them

if they do it wrong, or if they don't do it at all. But anyway, I realize that lots of people are working to try and improve things.

The bad news is that policy is not changing fast enough. Most agencies already seem to be in clear violation of the Executive Order. Sadly, the current Congress has gone out of its way to discourage declassification.

What about the future?

Last year, I submitted a FOIA request to the CIA asking for intelligence budget information dating back to 1947. Incredibly, the request was denied, on grounds that releasing even the very first CIA budget from 1947 would cause serious damage to national security. I wanted to write back, urging the CIA leadership to maybe take a night course in national security policy, so they could get a clue about what threatens national security and what does not.

But I realized that the CIA's denial of the request was actually more informative than the information that I had unsuccessfully requested. It reveals, I believe, an agency that is out of touch with reality and that is suffocating itself with its own security policies. Senator Moynihan wrote a famous op-ed a year or two ago, suggesting that the CIA is so bureaucratically entrenched that it will still be around 50 years from now.

My guess is that that is not correct. The very quality of bureaucratic entrenchment that makes the CIA and the rest of the intelligence community so resistant to change is also leaving them unable to adapt to new realities And those new realities are something wild. The outstanding fact about the future is that, for better and for worse, we are headed for a world of increasing transparency, in which the task of securing information is going to become much more difficult and, in certain cases, impossible. We are not going to have any more secret wars or secret programs on the scale of the Manhattan Project. That just is not going to be an option.

Sometimes, in dark moods, I doubt the value or necessity of criticizing government secrecy. Because, in a way, advocating increased openness is sort of like demanding that the sun rise tomorrow. It's going to happen whether I am in favor of it or not.

Why is it going to happen? The main reason is that, as a result of technological changes, the balance of power between individuals and government is shifting dramatically in favor of the individual. In a startling development that is not widely recognized, individual American citizens will soon have greater access to many types of intelligence--including imagery, open source intelligence, and even SIGINT--than the entire U.S. government did as recently as the 1960s. A few examples:

Commercial imagery satellites that are expected to be launched at the end of next year will provide high resolution imagery that is superior to any satellite imagery the government had prior to 1966. The imagery will be available in near real time--within a few hours--a capability that the government did not have before 1976.

As far as open sources are concerned, it is hard to overstate the explosion of resources that have become publicly available from around the world. It has become easier and easier to publish information, and more and more people are doing it, representing every imaginable interest and point of view. Even more important are the information processing tools that have now become publicly available. It is not too much of an exaggeration to say that intelligence analysis could soon become a personal hobby.

Even in the rather arcane world of signals intelligence, there are a growing number of amateur analysts. A new book by Steve Douglass provides radio frequencies for government and military facilities throughout the country. Security officials always have to assume now that someone is listening, even if the communications are encrypted, even if the facility is an unacknowledged one.

My colleague John Pike has prepared an introduction to many of these resources and their potential applications for public interest purposes that he calls Public Eye. It is available on the world wide web at http://www.fas.org/eye/. If you have web access, you may want to check it out. If you don't have web access, you need to get it.

Anyway, as a result of these new developments, the government's ability to generate and maintain certain kinds of new secrets will be severely curtailed. And I don't believe that this tide of openness can be turned back. The question is whether official security policies can adapt to new realities. In particular, the challenge is to identify the core of legitimate secrets with sufficient precision to allow a dramatic reduction in the volume of classified information, so the credibility of the classification system can be restored and at least those real secrets can be protected. Maybe that is too difficult, and maybe it is too expensive in the short term to cut the secrecy system down to size. That is the prevailing opinion in Congress today. But if that is the case, and secrecy reform is just not practical, then in my opinion the security system is headed for a state of anarchy. And that will not serve the public interest.

DOUGLAS PERRITT

Mr. Perritt was involved with Signals Intelligence in various capacities for more than 26 years before moving to the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence). This included 22 years at the National Security Agency in a variety of analytic and management positions, preceded by 4 years in the Army as a linguist. At NSA from 1985 to 1990 he served as the Chief of tthe External Affairs Division in the Office of Policy and from 1990 until 1992 as Deputy Chief of the NSA Operations Budget Staff.

In 1992 he went to OASD(C3I) as the senior advisor for Signals Intelligence. The following year he became Deputy Director of the Intelligence Systems Directorate within OASD(C3I). He became in 1994 Director of the Intelligence Operations Directorate within OASD(C3I). In March 1996 he assumed his current position as Principal Director for Information Warfare, Security and Counterintelligence, three of the directorates within the office of the DASD(I&S). In this position he is responsible for policy and oversight of Defense programs and activities related to information warfare; information, personnel, physical and industrial security; and counterintelligence and investigations.

THE INTELLIGENCE COMMUNITY: THE NEXT 25 YEARS

Douglas Perritt

I am pleased to be here to address this select group and to be a part of discussion of this important topic. Looking at the conference title: "Security Issues for the Next Quarter Century" gives me some pause. It is difficult to predict the future but, I believe, equally dangerous not to try.

I would like to give you a sense where I think the Intelligence Community is headed in the next 25 years. As most of you know, our office is charged with development of policy for intelligence and security in the Department of Defense. This gives us the chance to attend a lot of meetings, deal with daily crises and issues, and--occasionally--think about the next day. This conference and the topic now give me a chance to be a visionary.

In a way, we in the Intelligence Community feel as the Wright Brothers must have, when they pushed their canvas-covered biplane from their bicycle shop. It was this contraption they hoped would free them from the bounds of earth. Getting around *on* earth was a routine that had been perfected over many centuries. Taking to the skies was full of uncertainties. The Wright Brothers faced that challenge and lifted off from Kill Devil Hills. The world celebrated that achievement, but for the next decade or so, had no idea where this technology would lead.

In the intelligence world we face the same future: we were comfortable in doing business in a certain way. We now find ourselves looking toward a clouded future. Yet, we know we must climb aboard that plane.

We find ourselves still in the early years of the computer and information age. Like those who stood in awe at the beginning of the age of flight, we marvel at the possibilities, but are uncertain what these possibilities really might be, or where they will lead. More on this later.

The Cold War is over. The monolithic Soviet threat that drove our decisions on how and what to collect is now gone. The absence of this easily understood threat is unsettling to some because of the uncertainty it brings. In its place is a diffuse and multi-faceted threat.

We have many challenges facing us as members of the Intelligence Community. Not the least of these is the requirement to do more with less. We know that all budgets are subject to extreme scrutiny. We do not want to spend money needlessly. We want to practice risk management. In short, we want to retool and refine a system that has been working for the policy maker and war fighter for the past 50 years.

Two big drivers are at work in the Intelligence Community today. The first I've just mentioned: the end of the Cold War and the drive to reinvent the Intelligence Community. We have a charter to re-examine, re-engineer, and readjust to meet today's needs.

Just as we thought we understood that need to adjust, we were ambushed by the second driver, the Ames case. The aftermath of that case is still being felt throughout the community.

Congress has been involved in making sure that legislative input is heard. You have all seen or heard of the study of roles and missions of the Intelligence Community, conducted by the Aspin Commission, which became the Brown Commission following the untimely death of Les Aspin. Former Secretary of Defense, Harold Brown, published his report on the first of March. Shortly thereafter, both the House and Senate completed similar studies. All these studies look to change and to retain parts of the current system of gathering, analyzing and disseminating intelligence.

Meanwhile, we have, in John Deutch, a man who takes a very aggressive approach in restructuring the role of the Director of Central Intelligence. He is also keenly interested in the way in which the Iintelligence Community is organized, led and managed.

This is context. You wanted me to speak of the future, the next quarter century. Here goes.

I will not address organizational structures of the Intelligence Community 25 years from now. There may be many organizational changes, going far beyond the establishment of an imagery agency now pending, or the consolidation of production some contemplate.

Instead, let's start by thinking about the core of what we currently do and whether that central core will remain important in the future. Being able to provide the policy maker and the war fighter with information in a timely matter will still be the core mission of the community in 2021. We will continue to be the eyes and ears of national security.

Our primary goal for Intelligence in the Department of Defense is to provide the war fighter with dominant battlefield awareness. That means the commander will have at his disposal the most current, all source information about his immediate and long-range situation. The ways in which we acquire information will continue to evolve. Our most advanced technologies will be brought to bear. Additionally, the ready availability of enormous amounts of information in open sources will challenge our abilities to process and use it. Commercial satellite photography will probably be available to everyone worldwide in quantities and quality undreamed of today.

We must, however, have the ability to understand what we are seeing or hearing or reading. After all, Intelligence is information that has been processed and analyzed.

We will need human sources as well as technical ones. And we will still need individuals in the Intelligence Community who, with the assistance of computers, can manage the increased flow of raw material, and can make sense of it.

I see the Intelligence Community in the future being smarter, being more aware of developing situations. We will be able to provide real-time input to the Commander at all levels, to the decision maker. Today, we tend to step back and let the operators operate. In the future, as operations become more information dependent, intelligence may be even more integrated with military operations. This is the core of the national intelligence mission in 1996 and in 2021.

As we move from that core mission, I see the Intelligence Community working for other national security purposes in the future. We will be involved with coalition forces in joint operations. We will share intelligence with former adversaries as well as allies. These very teams may need to be revised. Intelligence will aid broad American national security objectives at home as well as overseas. We will aid the world in the development of data on environmental issues. We will assist in disaster relief operations by providing intelligence data to those who need it to assess damage. We will, of course, need to continue to safeguard our intelligence sources and methods as we perform these new missions.

I also see us having to deal with an emerging personnel security problem as we move in these directions. We will need to have assurances that the persons we select to be a part of this community understand what it means to safeguard or be a custodian of sensitive and classified information. We cannot rely on the hope that everyone agrees with the need to be secure. It is now more difficult than ever to get security awareness messages across, and to have them received well. We will need to communicate to our trusted employees that, even though the Cold War has ended, the need to safeguard has not. We will need to make it clear that espionage is not just another business deal between competing interests. It is a serious and very damaging crime.

We need to balance the pressures to manage risk--such as fewer compartments, less reliance on the polygraph, less stringent physical security--with pressures to prevent another Ames--with things like stricter security, tighter management practices.

We will need to address risk management. That means we will need to look at the possible outcomes of any course of action and decide which ones we need to guard against or plan for. If the Internet is seen as a key problem, and I think most would agree it is, then we must put resources there to safeguard our part of it. If the likelihood of some interest getting access to a highly valuable piece of information or equipment is seen as low, then we should devote less time to that threat.

We will need to discover and understand the impact that technology has and will have on our business. As I mentioned earlier, I believe we are only beginning to realize the potential offered by the explosion in information technology. We must learn to harness its power, but avoid becoming so reliant that information overload leads to slower, rather than better, decisionmaking.

Our reliance on information technology has another downside, as well. I believe that our counterintelligence and security professionals in the next quarter century will need to deal with an increasing threat of cyber-crime and cyber-spying. Our challenge will be to stay at least one step ahead of the millions of potential crackers and hackers who see us as fair game.

The definitions of classified and sensitive information will probably evolve. Again, there will be a struggle to balance the rights of privacy and the security of information. These may often be the same. We need to ensure that only the most critical information is classified. And I would imagine that a central core of classified information will become relatively small .

There is another side to the classification issue: we will also need to declassify and downgrade as much information as we can, as quickly as we can. Keeping it classified often serves no purpose and can cost money. I do not want historians in the year 2021 to be clamoring for release of information from the Korean Conflict or from Vietnam! We will need to bring automated processes to the declassification problem.

Our goal for an Intelligence Community in the 21st Century would be as follows: one that continues to focus on the policy maker and the war fighter, but that also provides timely information of value to the widest possible consumer base as the definition of national security continues to be refined. And, I would hope that the Intelligence Community of 2021 can be one that is a source of pride for all Americans. We need to restore the luster through hard work, and by cleaning up any problems, and continuing to serve the nation.

SCOTT ARMSTRONG

Mr. Armstrong is an investigative journalist and the Executive Director of The Information Trust. The Trust is a nonprofit organization devoted to facilitating freedom of expression in the U.S. and abroad, improving the quality of journalism, increasing accountability in government through access to information, reforming abuses of government secrecy, and protecting whistleblowers from retaliation. He founded the National Security Archive, which provides journalists, scholars, Congressional staffs, present and former public officials, other public interest organizations and the general public with comprehensive government documentation. He was the first executive director of Taxpayers Against Fraud which investigated contractors defrauding the government.

Mr. Armstrong is the author or editor of six books on various foreign, defense, intelligence and national security policy issues. He is presently working on a book on American national security policy. From 1976 to 1985 he was a staff writer for *The Washington Post*. He co-authored with Bob Woodward *The Brethren* and worked with Carl Bernstein and Bob Woodward as a researcher/writer on *The Final Days*.

Note:

Mr. Armstrong was invited to participate in this conference because of his record as a journalist. In the course of his remarks, he discussed at length a case currently in litigation in the U.S. District Court for the Northern District of California. The Defense Department has an interest in this case, although it is not a party. In an article published in the Washington Post on February 19, 1997, Mr. Armstrong noted that he served as a consultant to the plaintiffs in this case.

Mr. Armstrong's comments on this case, "The Lockheed Sunnyvale Case," which appear on pages 84 through 86 of the Proceedings are inconsistent with the view of the Department of Defense. Subsequent to Vision 2021, the judge granted the government's motion asserting the state secrets privilege to prevent the release of the classification guides Mr. Armstrong mentioned in his remarks about this case.

SCOTT ARMSTRONG, Discussant, SESSION II

We have some common features among the various perspectives represented here: Eric Biel represents a political entity, Senator Patrick Moynihan's Commission on Secrecy; Steve Aftergood represents the public interest community; Doug Perritt represents the government policy community; and I represent the journalist community. As someone said earlier this morning, "To make sense of the future, we need to make sense of the past." From each of these perspectives, we share concerns about the preservation of a free society, about protecting civil liberties and free speech, and we worry about how these concerns play up against the values embodied in the procedures we are discussing today.

What fascinates me about what Ted Sarbin has put together today is that we have an opportunity to be realistic about the past and about what can and should be done in the future. We are not here to talk about how much classified information we are losing through press leaks or if it is too much. We are not here to see if some of us would be satisfied if more information that is 50 years old were declassified sooner. And we are not here to talk about some naive notion that the government, like some enormously complex science laboratory, can be totally open.

We are here for an entirely different reason. We are here to talk about mutual goals of public trust and accountability within a tri-partite governmental system that is necessary to protect our nation state, a system which has existed through periods of great uncertainty in which the danger of tyranny was considered as great from within as it was from without, a system which was traditionally able to isolate secrets from a clearly (if not always accurately) identified enemy, a system in which secrecy could be effective, a system which existed before the interconnectivity of our global society.

Reference was made earlier today to Supreme Court Justice Potter Stewart's adage during the Pentagon Papers case, that "if everything is secret, nothing is secret," where disdain for the secrecy system becomes so strong that no secret is safe.

I remember General Richard G. Stilwell showing disdain for rigid secrecy and arbitrary compartmentalization. He told me that he thought that 95% of controlled information in government was unnecessarily controlled or over-classified and that made it difficult to control the other 5%. General Stilwell's point in his 1985 commission report on secrecy was that we cannot achieve a zero tolerance for security breeches when we have breeches occurring because 95% (he used a different figure but that's what he told me in a private conversation) of what is classified either should not be, or need not be, classified. And if we look at the effect of these unnecessary controls, and we look at the overlay of personnel security, I think we begin to see how some of these themes play out.

We talk about loyalty, trust, reliability. We are talking about a security system in which people lose their inhibitions about violating security procedures because loyalty, trust and reliability are missing. Doug Perritt made reference to "sensitive" and "classified" information. I take sensitive to mean that something might damage values about which an individual cares. We often find that government officials treat "sensitive" information with more care than "classified" information. Why? "Sensitive" has something to do, I think, with what we define as loyalty and the issues that surround our common-sense notions of discretion.

We have a broad definition of what intelligence does and where information relevant to an intelligent assessment derives. We are part of an information society in which we do not know the parameters. When we do try to control the flow of information it becomes increasingly more difficult. We have discussed tribalism and patriotism. I'm of the belief that loyalty depends on what team you are on. One is loyal to one's team. And if you confuse this commitment with patriotism, you are probably making a mistake. Because patriotism is not the dynamic force you see in Washington. There is a different focus for loyalty in the White House or even in different wings in the White House than there is in different government agencies or than there is in Congress or in a specific program or compartment.

I remember a Senator, a conservative Republican Senator, telling me some time ago that when the members of the Senate Select Committee on Intelligence were briefed on covert actions they often were not provided opportunity for real inquiry or debate. No question or comment they could make during the briefing would effect the covert actions about which they were told. There was really no recourse. The covert actions were effectively in motion. The committee members could do nothing to alter them or to stop them. The only covert action available to a U.S. Senator was to leak information about the administration's covert plan. That was their covert action, and sometimes they felt that such leaks had to be done in the interest of patriotism. And it was done in what they considered to be a responsible manner.

Well, contemplate that for a while. If this is what a conservative Republican Senator believes, it tells us about what you are going to have to do with the problems that you are up against.

THE COST-EFFECTIVENESS OF SECRETS: ARE THEY ALL WORTH KEEPING?

If you add to that concerns that Doug Perritt raised, you have an underlying concern about the cost-effectiveness of the secrecy system. Let's look at government national security secrecy as if it were one more weapons system. You have to build that weapons system in the context of a particular threat assessment. Your resources are getting ever scarcer for continuing the weapons systems you need. Increasingly, you have to justify yourself based on effectiveness. You have excessive costs which are acknowledged to be building to somewhere over $2.7, to nearly $3 billion. We all know that these cost estimates are really a very minor part of the over all costs of secrecy. If the effect of secrecy is to raise contractor costs by adding special fees for compartmented handling of information, what is the cumulative cost? If our secrecy system ends up arbitrarily silencing whistleblowers who could save the government say 20% of major contracts but will not be able to communicate the proper information because of unnecessary or inappropriate classification, then we may have added many tens of billions of dollars of secrecy costs to our operations.

The price of secrecy and the effectiveness of secrecy have become serious issues. If we were looking at it in terms of another weapons system, would this be a system that would get stopped dead in its tracks for being ineffective? People would say, "Well, wait a minute, what we are doing now just isn't working. We've got to rethink it. We've got to stop major portions of this and come up with something different." What would happen if it would cost us three times more today to equip our troops in the field? Suddenly everyone would say this is not a cost-effective way to equip troops. Well, that's the same issue when you put it in terms of secrecy? If we blind our decisionmakers by not giving them information because we over-compartmented the system, we end up having them ignore what good intelligence and information we do have, have we not adversely affected the cost-effectiveness right there? And is it possible we have so severely affected the secrecy system that it is no longer an effective weapon system?

If we begin to look at personnel security through this prism, many of our compartmented programs affect cost-effectiveness, particularly as we get into the contractor community where in fact the oversight becomes more and more reduced and government accountability is less. Are we able to recognize the difference between a disgruntled employee in a contractor program and a genuine whistleblower? How do personnel security programs deal with that same individual? The difference may not look very great if you are not concerned with the substance of what the individual is telling you, but if you begin to look at the way the person is treated, more often than not the personnel security framework is used to repress information and deny legitimate inquiry rather than put out accurate, complete and appropriate information.

INFORMATION, THE CURRENCY OF DEMOCRACY: ADDING VALUE BY ADDING SECRECY

All day long, we've talked about how we are part of an information society. The commodity of value is information. All of you intuitively understand that information is the currency of democracy. The efficient, free flow of information makes our country different from other countries; it is what makes the other democracies like ours different from the other countries in the world. Our system works very well, but I've found that information tends to be more valuable when it's secret. Is secret information necessarily intrinsically different? No, it's more valuable because it has a cachet, because it has a different commercial use, often just because it is secret.

As a journalist I can put information on the front page of the *Washington Post* if I can assert that it is secret and that the government doesn't want the reader to know about it. The same information published in an open report often hasn't got a prayer of getting in the newspaper, much less getting onto the front page. One would have to invent an additional, "secret" news source to get it into the paper.

Today, we begin to look at the added value to information, the ability to manipulate information for different uses. Such value becomes even greater as the areas in the special access programs which permit us to take and crunch information from several different programs such as undersea acoustical detection, infrared detection and imaging radar data, and come up with specific conclusions. The refinement of the context in which the information is being controlled becomes more important. The user becomes more aware of the importance of the information. If you begin to look at the value added to you as a customer or to the government from within a particular program, you can begin to look at what it is you are trying to protect when you write a security classification guidance in the first place. If you assign value to the information and then ask why it is that a particular individual has a need to know that information, can you begin to develop an appraisal of the cost-effectiveness of secrecy across programs? I doubt it. And yet it seems that that's precisely what the government has undertaken now, to begin to look across program levels and put common denominators, common procedures, common abilities to deal with these same of questions. Maybe there needs to be different approaches to different kinds of secrets.

THE VALUE OF "NATIONAL SECURITY SECRETS" V. THE VALUE OF "POLITICAL SECRETS"

Steve Aftergood very thoughtfully talked about different kinds of secrets. Political secrets, bureaucratic secrets and genuine national security secrets, as he would refer to them. I am reversing the order, but for a purpose. What's interesting to me is the secrets that are most valuable to you, by and large, are the genuine national security secrets which tend to be technical or very specific in nature. These include sources and methods. But this category tends also to be, speaking frankly, the least interesting and valuable to

me as a journalist, and I suspect the least interesting to most national security decisionmakers and political players.

The secrets which are most valuable to journalists--and, I submit, to presidents--tend to be political secrets. I would suggest that included in political secrets are many examples of analytical intelligence but without any references to sources and methods. These are most valuable to journalists--and to presidents--because they are a snap shot of our perceptions of what was going on in the world. The more secret it is, the more valuable. The perception of reality at a given moment may be more important to the political dynamic in Washington than the actual reality of what is going on the world (which involves sources and methods.)

This suggests to me that sometimes there's an overlap in our objectives. There are of course analytical products that include information that could compromise sources and methods or that comprise information that would be "sensitive," to use Doug Perritt's terminology, although not for very long. It's very rare that you have information in which we journalists place a high regard that is truly "sensitive." And in such instances, it almost always comes from a covert operation involving very sensitive sources and methods where the crown jewels are in fact overlapped with the information that is most valuable to the journalist. The overlap in objectives comes from the simple fact that most of what journalists want the most is what you should want to protect the least.

THE PRESENT THREAT ASSESSMENT & SECRECY PRIORITIES: WHO CAN EXPLOIT OUR SECRETS

If you begin to think about the tension between where and how most personnel security resources are spent and where the actual damage is most likely to come from--those most able to exploit compromised information--you may find that it is easier to identify which tasks and adjustments should be given priority. We must look at the level of effort put against those tasks in the past, the resources devoted to keeping certain information secret in the manner about which we've been talking about all day long. I think that there is an implicit hierarchy here. If you look at the way the government as a whole is organized--not just your jobs, but the government as a whole--there is a very interesting matrix which correlates the classification and the clearance systems in terms of why particular personnel groups and programs get the most attention. Let's do a threat assessment of your target groups, a look at the characteristics of the organizations which the government appears to believe might most successfully exploit information you are sworn to protect.

Public enemy number one--the group from which your bosses most want to prevent getting classified information--is the public. That is to say public interest groups such as Steve Aftergood's and such as the press. These are the top targets of your security systems. More of your energy and resources in fact are put into protecting information from disclosure to these groups than any other. I find that startling.

The second-level foe is the Congress, the committees which can provide oversight and the independent representative who can haul your boss in for an accounting of what is going on.

At the third level are those offices and agencies inside the federal bureaucracy that have accountability functions--OMB, sometimes the White House, oversight boards, and others who can ruin you organization's day or year.

The fourth-level enemy would be the other military services and national security agencies. If you're in one military service, then the other services are a distinct threat. They will compete for scarce resources and will spoil your program's head start. As a matter of fact, Peter Saderholm suggested to me that the compromise of inter-service information might be regarded as the number one threat.

Next, fifth down the line, come true foreign foes. But there are fewer foreign foes who are able to exploit the political and technical information you protect so these foes may even fall down to a lower priority these days.

Sixth on the list would be foreign allies, although they may actually be moving up the list as your senior officials become more concerned about protecting information from their ability to exploit congressional supporters and corporate interests. Ask yourself, "Are we more concerned about our allies getting and exploiting certain classified information these days?

Seventh, we certainly have an interest in would-be terrorists, but how effectively do we block information from them? What is the cost-effectiveness of the information that they're seeking and our ability to prevent them from getting it, to really devote resources against them? I don't really know the answer to that. In fact, that may be one of your areas where an appropriate panelist can address the question later today or tomorrow.

Eighth, contractors--internal compartmentalization. Protecting very sensitive information for very good reasons because of compartmented concerns about information flow within organizations.

This hierarchy matches the deployment of our personnel security and classification system assets. And yet which of the major compromises of secret information in recent years come to mind as having been of the greatest concern? Do these match that allocation of security resources?

A friendly government co-opts an American citizen who penetrates a variety of intelligence programs inside the defense community.

A contractor employee walks out the door with classified manuals and delivers them to Soviet intelligence.

Career military officers deliver technical information and ciphers to Soviet intelligence.

A CIA careerist, Aldrich Ames, systematically collects the most precious Humint information and systematically provides it to Soviet intelligence, at the same time that a relatively new CIA operations officer loaded with pre-deployment Humint briefings walks out the door and shows up in Moscow.

Ironically, none of these cases involves the areas to which personnel security presently seems to be devoting its major resources. You are expected to plug all gaps, to establish zero tolerance. Yet, we know that the ship of state leaks from the top; this must be your major frustration. It is unrealistic for high-level government officials to expect you to do the impossible, to hold information within confined parameters when there are compartmented programs involved which are very controversial and are being debated at the highest levels of government. You have enormous extra expenses to clear every single riveter on a project and to keep checking on each employee from beginning to end. With all these overburdened resources, for the top brass to expect you to keep this zero tolerance going, they are being unrealistic, particularly when the leaks come from the top.

We as journalists know this principal. While we often do get information from people who are not on the highest level, in the end the right information, the perfect quote, the authoritative generic source is going to be somebody with very high-level access. We know that this is somebody you're not going to pull in for a quick polygraph; most often it is somebody who's going to be telling you to polygraph other people.

LOYALTY MEANS MAKING SECRETS RESPECTABLE

It's in that context that Eric Biel's comment about making secrets respectable becomes so poignant.

If you want people to respect secrets, you must make secrets respectable. This point has to do with the trust relationship between government institutions and the individuals who work for them.

From the point of view of a journalist, everyone in government will talk about something that they technically should not discuss. But the higher the person in government is, the more likely that seems to be true. At the highest levels, government officials will talk (at least on background) about almost anything to some degree. And I think this tendency tells you a lot about your job and what it is you're protecting against. Particularly in the past decade as hostile enemies who can exploit technical intelligence begin to disappear, everyone from their individual, different points of view has to seriously ask themselves: "Who is it that personnel security is protecting information from? What is it that we want to have protected? Who can exploit what information and to what degree? Who is it we want to adopt certain practices to deny others the protected information? Do we do this by increasing the individual's loyalty? If so, how? Is it

loyalty to country we seek or loyalty to the team? How do we reassess the value of a particular sort of information in relationship to its ability to be exploited. And then how do we reassess the value of the very specific and often limited information within a particular individual's range of access? Are we concerned about them because they can and might compromise a national security secret or are we concerned about them because they might compromise a political secret?

As a nation, we obviously have deep--perhaps even ultimate--obligations to human intelligence. In fact, no journalist fails to understand that the government must have the deepest obligation to human intelligence sources. Although we as journalists sometimes probably seem indiscreet, we make similar guarantees to our information sources. Journalists will go to jail to protect our Humint sources, so we certainly understand your commitment to protect your Humint sources. In other words, even journalists respect secrecy if its purpose is respectable.

What I think is implicit in both Eric Biel and Steve Aftergood's comments was a notion of building respect for what the system is truly required to do. But the essential ingredient here is to concentrate on that genuine part that has to do with human intelligence sources. From the point of view of many in the Congress and inside public interest organizations and of journalists, you are headed in the right direction if you concentrate on keeping secret respectable secrets. The good news is that if you concentrate your resources on protecting only that which General Stilwell would say requires protection, you are about to have a technological advantage in clearing the needlessly and inappropriately classified information out of the system.

TECHNOLOGY IS ON YOUR SIDE: ELECTRONIC CLASSIFICATION GUIDES AND TRACKING SYSTEMS

You are now entering an era where you will be able to create electronic classification guidances. In an earlier session, we talked about the difficulty of expecting people to refine the terms of classification guidances on the front end. I believe as painful as this prospect may be, you will find this a necessity. Soon you will be embedding metadata into a classified document so that each item of information classified in the document will be tracked electronically to an electronic classification guide. Thus every single item classified in the document will have a direct electronic tie to an individual authority within a specific classification guide. Conversely every document or piece of information classified under any one section of any classification guidance can be traced. Thus when the guidance changes (when the classification changes or becomes obsolete) all the documents classified under the guide within the system will automatically be changed, or at least will be changeable, when they are plugged back in to an authorized retrieval system for reuse later.

Similarly access compartments will be electronically controlled. If your access compartments, your access levels, are authorized electronically, individuals whose clearances have changed or lapsed won't be able to get to documents they might have

been able to get to the day before. Some of you may note that this is not in fact an advantage; it may become a nightmare to have to track individual access transactions. You will be able to see who is looking at what documents at great levels of detail. But all of this, I think, is implicit in our question of, as you approach this system, do you want to try to apply it broadly or do you now recognize the need to narrow the applicability of these new technologies to protect only that which truly must be kept secret? The system seems to us on this stage--some of us more than others probably--to be badly broken at present. There are too many examples where you must say on behalf of agencies of government "we will have to pursue multiple and contradictory goals at the same time simply because we are at present confused about what it is we want to protect."

THE LOCKHEED SUNNYVALE CASE

The difficulty is compounded when agencies of the government are not only confused about their goals, but they can't require accountability of government contractors because they can't get effective audits inside a compartment. Let me give you an example of such a problem writ large.

At present, as we speak, there is a scandal which has been percolating for several years through the federal district courts of Northern California. Whistleblowers inside Lockheed Missile and Space Division in Sunnyvale, California, came forward in the late 1980s with information about personnel misbilling. After the contractor and the military customers failed to act on the information brought by the whistleblowers, they filed a lawsuit under the False Claims Act on the government's behalf to recover from Lockheed roughly, at the outside figure, $1.5 billion for misbilled time to Sunnyvale contracts with special access programs run out of NRO, NSA, CIA, Air Force, NASA and other program departments. The Lockheed defense was at first that the alleged misbillings didn't occur. Now the defense has become that employees who were in "icebox" status[1] were allowed by government warrant holders to move between compartments to work on other programs for which they were also not cleared.

The Justice Department lawyers who reviewed the case to see if they wanted to take over as lead counsel elected instead to let the attorneys for the whistleblowers pursue the case. In their view the recovery from the case would be "trivial" because even if Lockheed had billed the wrong program or the wrong account (a program account instead of an overhead account), the government would have to compensate Lockheed out of one pocket to recover money in another pocket.

The whistleblowers' lawyers continued the case anyway, discovering as they went that in fact which accounts were billed made a considerable difference to the taxpayer and a great deal of difference to Lockheed's profitability during this period. By billing other

---

[1]Awaiting compartmented clearances and unable to work on classified work within the program to which they were assigned until that clearance arrives, i.e. "in the icebox."

accounts for personnel who were supposed to be in the "icebox," the acknowledged level of billings in question is potentially $500 million which with treble damages means a government recovery potentially of $1.5 billion. I think that we all agree that $1.5 **billion** is not trivial. Particularly if that represents a fraudulent billing to the costs of maintaining compartmented security at a facility like Sunnyvale.

Early on in the case, the same Justice Department lawyers who had said the case recovery would be trivial raised questions about whether any contractor personnel billing information could be provided to the whistleblowers' lawyers without compromising the obviously highly sensitive compartmented programs within which they worked. To everyone's surprise the program customers said that the information could be codified so that it could be used in the case--and ultimately in court--without disclosing the nature of the specific programs or such possibly sensitive data as the cost of each program. That cooperation led to the conclusion that the possible fraud was sufficiently high that it was non-trivial.

Last year, the Justice Department objected on its own to the possible disclosure of classification guides to assist the whistleblowers' lawyers--who incidentally are uncleared. When that happened an interesting possibility presented itself. The whistleblowers' lawyers proposed that rather than declassify a great deal of information from what they agreed were highly sensitive compartments, they would designate a retired high-ranking government security expert--in this case former deputy assistant secretary Maynard Anderson--as their representative. Anderson, who retains active clearances to most if not all the compartments in question, would review the documents within the compartment and decide what was truly necessary for the case to go forward. The plaintiff would drop its request for the remaining materials. Anderson would work with the government's program personnel to see if there were not ways to redact materials with some indexed codification that would allow the cases to be used in court without damaging the national security. At no time was it ever proposed that Anderson would have any authority to declassify anything or to discuss any classified information with anyone not cleared for the relevant compartment--including the whistleblowers' attorneys. The judge thought this was a terrific resolution of the problem since it would allow the government to serve its otherwise conflicted interests simultaneously by protecting the national security while stopping allegedly on-going fraud and recovering any improperly billed costs. The judge then jawboned the Justice Department into drawing up an agreement to allow Anderson into the compartmented materials.

What happened next is astounding. The Justice Department on its own, apparently without the support of the programs involved, drew up an agreement for Anderson to sign that would not permit him to discuss whether information in the compartments was properly classified or not with anyone outside the compartment including higher level DoD authorities, the Information Security Oversight Office or even the judge in the case. Anderson was put in the position of not being able to report improper classification activity, a reporting obligation his clearances require him to observe. When Anderson could not sign the agreement as drafted by the Justice

Department and Justice refused to let the materials sought under discovery be produced, the judge insisted they file a state secrets affidavit.

In order to prevent the case from going forward, the Civil Division of the Justice Department has gone so far as to put affidavits in front of CIA Director John Deutch and Deputy Secretary of Defense John White which assert falsely that the whistleblowers' discovery requests which were actually for classification guides were instead for the underlying information covered by the guides. They also told them that the whistleblowers and the court had proposed that Anderson would act alone as a special master making declassification decisions while on the payroll of the whistleblowers' legal team. This was never proposed, but these false assertions got the state secrets affidavit signed.

The Justice Department set up a strawman and then knocked him down. In fact, I think they missed the opportunity everyone has been seeking since the Joint Security Commission headed by Jeff Smith noted that there were severe security abuses in compartmented programs. The Justice Department apparently thought this would be a bad precedent to have an independent expert who might be asked by a judge if the classification decisions were proper and necessary. The Justice Department thought too much was at stake. Yet this is an intriguing proposal that amounts to introducing a civil version of CIPA (the Classified Information Procedures Act). It's an interesting metaphor for a solution to a whole raft of problems in the long run.

Those of us on the outside like journalists have always wanted to get all the information on the inside. Gradually, we've come to understand that's not going to happen. As we become more technologically sophisticated, we have to understand that what we and all citizens are really after is accountability within parts of the government into which we cannot regularly probe. And we're not going to get that by having every piece of information. So in this particular case the plaintiff designated a person who recently left government, a person who still has his compartmented clearances, to review the information in terms of what information is irrelevant, what information is relevant and how records dealing with personnel billing, not with the substance of these programs, can be codified in a way that it can be brought up and used in a courtroom without damage to the national security. The judge considers it reasonable, I think most of the program personnel consider it reasonable. But the Department of Justice doesn't want to do it.

Why? Because they don't want to create a precedent in which Maynard Anderson --or one of you after your retirement still with clearances--can become an expert and end up in court with a federal court judge deciding whether you can testify in unclassified form about classified matters because that's what is necessary to establish accountability in the system.

CREATING CONTEMPT FOR THE SECRECY SYSTEM V. REESTABLISHING TRUST

Well, think about the proposition this case represents--that the government can meet several of its obligations at once without violating the others: program accountability, protecting secrets, recovering money stolen from the public, allowing the courts to provide justice to civil plaintiffs. But the Justice Department doesn't want to take the chance that a federal court may obligate the government to do this the next time. It is decisions like this that reduce respect for the secrecy system you administer.

As a result, you have the degree of the lack of trust between government and citizen that now exists. That trust has to be reestablished. I am willing to live with the notion that those of us who are on the panel, with the exception of Doug Perritt, are never going to be inside the compartments of special access programs. But we have to have some process that we can trust to be sure that some independent person will be able to inquire into those compartments. Those of us on the outside do not trust Congressional oversight of the defense and intelligence communities to hold these programs accountable. I think we heard themes constantly today that there is an obligation that you each have to restore citizen trust in government. We are not just talking about government and contractor employees trusting the system and because they trust the system, no one has to worry about whether they are going to leak or whether they're going to compromise programs. We're talking about trust in a broader sense, trust which is based on the fact that a finite series of proposals, of mechanisms for accountability within secret programs can be put into place. Procedures can be adopted which will yield corrections where there are abuses within the system. If you find those mechanisms, you will find your job to be considerably less difficult. You will find for, example, whistleblowers will become your allies rather than your enemies.

OPENNESS AS PARADIGM

One last point: Openness. Openness is why some societies thrive. We live in an open society. We participate in an open debate. As a society, we value openness for its own sake. Our scientific community's openness presents us with enormous advantages that allow us to move more rapidly along technological paths to the future. Those societies which are not open operate with severe disadvantages. This means that our principal societal advantage--openness--is at conflict with your principal tool--secrecy. You must understand that conflict. You will want to be very careful about how you manage where the boundaries between the two are.

There are some among us who think that if you get to an era of radically reduced secrets, you have reduced the instances of disloyalty and of treason. If there were no secrets to compromise, there would be little about which to be treasonous. But you don't have to do away with secrecy to harness loyalty. However, you do have to listen carefully to what is being said within the confines of the system. You have to create mechanisms to allow for an open discussion within a bureaucracy. You must allow

people to compare their trade practices, to vent about the problems that they have uncovered on the inside, within the confines of compartmented secrecy--whether it's scientific or technical or analytical. They must be able to compare the practices and standards they see internally to what people are doing outside their compartment.

As you allow employees to do this, you begin to be able to distinguish, then, between the simply disgruntled employee and the true whistleblower. The disgruntled employee may be someone you can marginalize and make sure he/she doesn't cause damage. The true whistleblower is someone whom you want to keep in the system and whose information you may want to exploit in order to correct the problem internally.

SESSION III

MAYNARD ANDERSON

Mr. Anderson is currently President and Managing Director of Arcadia Group Worldwide, Inc., consulting in matters of national and international security. Among his other current activities, he is Chairman of the Board of Directors of the National Intellectual Property Law Institute.

Mr. Anderson's last position in government was Acting Deputy Under Secretary of Defense for Security Policy, with responsibility for providing advice in the development of overall defense policy for international security programs, national disclosure policy, special access programs, NATO security, the Foreign Disclosure and Technical Information Systems, and related security policy automation systems.

From 1988 to 1991 Mr. Anderson served as the Assistant Deputy Under Secretary of Defense (Counterintelligence and Security). From 1982 to 1988 he was Director for Security Plans and Programs, Office of the Deputy Under Secretary of Defense for Policy, where he reviewed and formulated policies that govern DoD's security practices and programs.

PERSONNEL SECURITY: NOW MORE IMPORTANT THAN EVER

Maynard Anderson

FOREWORD

In *Walden*, Thoreau quoted from The Analects of Confucius:

> "You who govern public affairs, what need have you to employ punishments? Love, virtue, and the people will be virtuous. The virtues of a superior man are like the wind; the virtues of a common man are like the grass, when the wind passes over it bends."

This conference should guide some of you who govern public affairs and whose responsibility it is to determine how best to ensure the integrity of those who keep our nation's secrets. At least some of you will agree with Thoreau, Confucius, and other wise men that attempting to acquire employee loyalty by fiat, or by the threat of prescribed punishments for disloyalty, will not change their behavior any more than regulations against employee theft and espionage have prevented those actions.

Modern governors of public affairs would risk the label of "politically incorrect" should they classify those subject to their authority as "superior" or "common." Indeed, in terms of personnel security, in a government context, all men and women are created equal. Access to classified information is not granted on the basis of rank or position, theoretically, at least. In the sense of the analects, however, for modern day purposes, leadership can substitute for "superior," and we can speculate about how others will be affected by applications of influence, power, corruption; or how some are vulnerable to threats of a stronger force.

Leadership in this security process is increasingly important because you who govern public affairs are losing some of your influence. Writing in the "Executive Summary," The FEIAA newsletter, in April 1996, FEIAA president Bruce Johnson, cites *Washington Post* surveys that describe declines in participation in neighborhood associations, churches, PTAs, and other civic and community organizations. Weakening interpersonal and community bonds seem to be statistically associated with a weakening relationship between the people and their government. The surveys indicate that Americans mistrust government and are alienated from it because they increasingly mistrust each other. Included in those who mistrust government are government workers.

Robert Bly (*The Sibling Society,* Addison-Wesley Publishing Co., 1996) writes that we are a nation of squabbling siblings who tolerate no one above us and have no concern for anyone below us. We have a spiritual flatness. Internally we no longer want to be good; we want to be famous.

At Woodstock, according to Bly, the high school students won. They won a battle against what Jules Henry (*Culture Against Man*, New York, Random House, 1963) called "The Indo-European, Islamic, Hebraic impulse-control system." The old structures of the impulse-control system have loosened; the nation relaxed; the Beatles happily sang about living in a yellow submarine.

Bly asks, "How did we move from the optimistic, companionable, food-passing youngsters gathered on that field at Woodstock to the self-doubting, dark-hearted, turned-in, death praising, indifferent, wised-up, deconstructionist audience that now attends a grunge music concert?"

From the perspective of those of you who have responsibility for personnel security in the government, that question is a starting point in understanding that changes in our personnel have taken place, are taking place, and must be addressed. It is no longer enough to say that we should be subject to rules that require responsible conduct when there is an attitude among many that the only requirement is obedience to the rules they like.

In the following paper submitted for consideration by this conference, I have reviewed some old and continuing issues. And I have speculated about some ways in which we might transition from the traditional ways of formulating security policies and procedures followed by routine implementation sort of by-the-numbers, to a more modern, flexible, in-the-environment, application of security as its needed.

INTRODUCTION

Security professionals understand that protecting secrets is dependent on the abilities and intentions of those to whom the secrets are disclosed and entrusted for safekeeping. Security professionals have frequently reviewed and evaluated this human aspect of asset protection that is called personnel security, but not much has changed in its administration over the years.

The personnel security programs continue to require that candidates for positions of trust provide information about themselves; that information is used as the basis for investigations that confirm or rebut the submitted history. Investigative results are used by adjudicators to form opinions as to the candidate's reliability, suitability, and eligibility for a position which will theoretically, at least, through its requirements, test the abilities and integrity of the individual selected, and the validity of the investigation. Thus, the only measurements of the effectiveness of the personnel security process occur after the process is nearly complete. This assumes that some semblance of continuing evaluation is part of the process and will provide some continuous measurement.

More often than not, if the investigation produces no disqualifying data, the candidate is selected for employment or cleared for access to classified information, or both. In such cases, the process results in adjudication by exception; if no bad

information is uncovered, the candidate gets the position. It is easier and quicker that way. More cases are completed in a shorter time and all concerned can get on with their business. Despite the fact that unreliable people, irresponsible people, and untrustworthy people are selected for positions where valuable things and information are at risk, the efficiency of the process has long been more important than obtaining positive evidence of trustworthiness, the real objective of the personnel security program.

It is as impossible to predict future happenings as it is to predict human behavior. However, a critique of past and present programs leads to speculation about possible future requirements that will have some impact on developing a progressive personnel security program for the twenty-first century. A review of issues in this context also points to some other ways in which the program must be managed in the future. This paper includes a critique along with ideas for use in next century programs.

One explanatory note--the opinions expressed in this dissertation are mine and subject to change without notice. The proposals for future actions are not radical but realistic in terms of possible bureaucratic acceptance. Forecasts of security practices that will be employed early in the next century are based on security's historical position of being at least one generation behind reality. Technical capabilities exist today that make it possible to immediately implement every proposal that involves technological support.

No doubt there will always be a need in bureaucratic institutions for formulation of some sort of basic policy framework. However, emphasis on security policy-making will diminish because new technological applications have solved many of the old problems surrounding protection or safeguarding and transmission of information. Technological abilities to manage information domains as they will be used in the Defense Information Infrastructure, for example, will enable more effortless control of sensitive information and personnel access to that information. Policy-making will be more decentralized as well because of wide-ranging and rapidly evolving operational requirements of both Defense and many civilian agencies of government.

Owners of information must focus more on individual or group, soldier and small unit, for example, and emphasize security thematics that have begun and will play out over time. Security implications of some of these themes are discussed in this paper: Information power; information distribution; individual isolation and the consequent shifting responsibility for access control; technology power; the diminishing importance of the bureaucracy; regulatory incontinence - no logic, no enforcement; more disciplined enforcement by statute; and consolidation of information warfare. All of these support the central theme that security is not an abstraction, but a management issue.

BACKGROUND

There is some doubt that a system crafted in 1952 to deal with loyalty for Federal employment is still viable. Periodic examinations of the program by federal officials have been based on premonitions that the program could be more effective.

The Hoover Commission Report of June 1955, advised that, "one flaw in the present system ... seems to be the absence of a general plan for a periodic review of the security status of every person after employment, to guard against the possibility that some employee who was completely dependable and honorable when starting work might have changed character, fallen from grace, or succumbed to alien blandishments or some personal weakness."

In 1982, a "select panel" reviewed the Defense Personnel Security Program. It concluded that:

- The program does not ordinarily catch spies.
- An initial investigation is rarely the basis for denial.
- Most derogatory information comes from sources other than the investigation.
- There is not a universal effective system of continuing personnel observation and evaluation.

Those descriptions of program faults are too eloquent and succinct to have been ignored for so long.

The general conclusion of the 1982 select panel was also an indictment of the program: "While the program aims to prevent penetrations of the DOD by hostile intelligence, the most tangible results are to grant security clearances to persons whose past actions indicate they are reliable, stable, law-abiding and free from factors that would make them vulnerable to approach by hostile intelligence, and to deny clearances to those who do not meet these tests."

Other government reviews under the auspices of various committees and working groups of the Intelligence Community, the Office of Personnel Management, and the Department of Defense, continuously wrestled with issues like investigative scope, different and redundant requirements among agencies of the government, use of the polygraph, education and training, clearance and access reciprocity among the various authorities, and due process.

The Stilwell Commission[1], the National Industrial Security Program Steering Group[2], and most recently, the Joint Security Commission (of DOD and CIA)[3] all considered personnel security changes within their deliberative charters.

The Stilwell Commission prevailed upon the Secretary of Defense and succeeded in rationalizing the establishment of the Defense Security Institute to train personnel; the Defense Polygraph Institute to train personnel and conduct research; and, the Defense Personnel Security Research Center (PERSEREC), to conduct research. For the first time in U.S. history, there was formal recognition of the need to support program changes with empirical data instead of mythology and folklore.

The bureaucracy has not responded enthusiastically, however, in providing funds, staffing and other resources to meet personnel security needs. Despite lethargic executive reaction, PERSEREC, as an example, has produced significant, tangible results for immediate application in the areas of prescreening, espionage motivations, investigations and adjudications analysis, and credit and financial records acquisition.

In 1988, the Rand Corporation asserted that there is no clear statement of goals of the program beyond *the need to ensure that only the most trustworthy and loyal individuals are engaged in Government service.* (Emphasis added.) That is a puzzling criticism because it would seem that any other goal of the personnel security program would be superfluous at least, and distracting from Rand's recognition of the program's basic objective.

Implicit in the criticisms of the various groups that have analyzed the personnel security program is a conclusion that the process has become more important than the results. For example, much effort has been expended in unsuccessful attempts to achieve uniformity in the proper application of due process. Even Supreme Court Justice Antonin Scalia, quoted in the *Washington Post* on June 24, 1994, said, "I believe that the process clause guarantees no substantive rights, but only (as it says) process." Additionally, it is improvement of the process that causes continuing examinations of such concerns as the validity of investigative requests; the validity of elements of investigations; and the efficacy of adjudicative guidelines and adjudicator's training, to name a few.

The history of the personnel security program does not demonstrate that it has ensured the employment of people who are aware of their security responsibilities. Nor does the program's history indicate strong and continuous determinations of the rationale for individual actions of trust betrayal. The program has done little to convince its constituencies that proper behavior in support of the national security is necessary. Security has not become an accepted pattern of behavior. Personal accountability of custodians of classified information has neither been established nor enforced.

To the contrary, personnel security has been weakened by some government policies that fail to ensure that competent officials have made rational decisions about what kind of information should be protected and how much of it should be safeguarded. Government policies that emphasize extraordinary physical safeguarding measures for too much over classified information detract from personnel security by diverting attention from human factors to protective measures like high walls of concrete and steel and automated access control systems. Government policies that stimulate a lax attitude

inspired by the trend toward lack of accountability for classified information by cleared personnel damage the personnel security program. Personnel who are given access to classified information without an accompanying requirement that they take responsibility for its protection and its disposition by making an accounting for it, cannot be blamed for thinking that the government doesn't care about its protection. These policies and practices are contradictory to the fact that personnel security is the most important element in the security program of any organization in which security is necessary.

As program history has placed focus on how the system works rather than on who is affected, process has triumphed over product. Program procedures and emphasis have not changed commensurate with the changing attitudes, values, mores, and beliefs of those most influenced by program application. A connection has not been adequately established between "personnel security" and each person touched by its provisions. The program hasn't recognized that people change and react differently in different circumstances.

Program examinations since 1974 have periodically and consistently identified some of the same procedural problems, but the security performance of our government and our personnel has been lower than our expectations.

CONTINUING ISSUES

Personnel security has always been based on the presumption that its investigative and adjudicative procedures and techniques employ valid predictors of human behavior, and that those predictors enable correct judgments concerning future behavior. But, there has always been a question as to whether those predictors lead to the proper determination that someone is trustworthy. Until quite recently, for example, it was not believed that it might be important to know how individuals view themselves through introspective techniques like in-depth interviews, psychological examinations, and polygraph examinations. Nor was the environment in which personnel needed to operate considered very often when, in fact, the impact of the environment on its inhabitants might be just as important in affecting behavior as the individual's inherent traits, characteristics, and inclinations.

The objective of a background investigation is determination of a person's loyalty and suitability for a position of trust. Occasionally, there has been greater emphasis placed on life styles than on loyalty. Care must be taken to balance those objectives. Recall the example of convicted felons who were prisoners in the United States and who were released on the condition that they perform military duties during World War II. I call it the "Dirty Dozen Dichotomy," while Roger Denk, PERSEREC's director, calls it the "Penal Paradigm." There were countless examples of heroism and bravery on the part of those prisoner-soldiers, which indicates that some of them, at least, were loyal to their government and their comrades despite their lack of suitability for a position of trust involving the handling of classified information or things of value.

In adjudicating someone for access to classified information, it may well be that the most difficult problem for the adjudicator is to judge people by the norms of society rather than by his or her personal standards. An adjudicator's experiences along with inherent or learned prejudices color the interpretation of the facts under review and may result in judgements that have little basis to predict future behavior. Personnel security adjudication requires the prediction of human behavior on the basis of past performance. Recollections of their past performances by subjects of adjudication are fallible as well.

The English writer L.P. Hartley said, "The past is a foreign country." And, one of the great American writers, William Maxwell, comments in a couple of different ways: In *Billie Dyer and Other Stories*, he writes:

> "In the attempt to retrieve the past, we create it anew, inventing as much as we remember."

In *So Long, See You Tomorrow*, he writes:

> "What we, or at any rate what I, refer to confidently as memory--meaning a moment, a scene, a fact that has been subjected to a fixative and thereby rescued from oblivion--is really a form of story telling that goes on continually in the mind and often changes with the telling."

Admiral Crowe, departing from the JCS Chairman's job, commented that retirement is that time in your life when the recollection of things that never happened becomes more vivid.

Nevertheless, the history of someone's actions has become the basis on which we attempt to decide the future performance of the person.

CONTINUING AND MORE CURRENT ISSUES

This issue list is lead by threats--threats to personnel and threats by personnel, the latter being of most concern to us in this context, perhaps.

The perception of threat changes and recedes occasionally as the United States defends against different kinds of adversaries, new potential adversaries, and friends who are economic competitors. These external threats change often. Today's enemy is tomorrow's friend, and vice versa. There will always be those seeking information to gain a strategic or tactical advantage, or a technology edge, who will find vulnerable personnel who possess something of value and attempt to obtain it from them. The internal threat from cleared personnel motivated to do harm does not change very much over time.

The internal, personal threat comes in many forms and as categorized by Michigan State University Professor David Carter for PERSEREC[4], may include:

- persons who are unhappy on the job in general.
- persons who are unhappy with the location of their assignments, particularly if they are perceived to be "off the beaten path."
- persons who feel they have been overlooked for promotion or merit salary increases.
- persons who feel they have been overlooked for commendations and awards.
- persons who do not feel they have been compensated for their contributions to the organization.
- persons faced with personal financial difficulties or stresses.
- persons facing personal problems, particularly if they feel that the way out of the problem is to escape, or that it is possible to buy themselves out of the problems.

Clint Schnekloth, a senior student at Luther College last year, rendered a somewhat more general and philosophical description of a personnel security threat in a classroom dissertation quoted here in part:

> "There is a threat to national security that is much more eminent (sic) and pervasive than the deficit, or weapons stockpiles, or bureaucracy. The greatest threat to the security of any nation is very simply human nature."
>
> "If we are to fully realize what the true threats to national security are, we must acknowledge that they have, as their source, the fallenness (sic) of humanity. All problems that we deal with at the national level originate out of the hate, pride, greed, and sin of humanity."
>
> "The question--how does human frailty play in 20th Century American society?" Or, more important, how will it play in the 21st Century?"
>
> "Society is in transformation. We define ourselves in terms of the groups we join, the beliefs we hold, the choices we make. The individual may be becoming the most important unit in our society."

Schnekloth posits that the result of increasing importance of the individual is societal fragmentation: for example, increase in divorce rates because individual interests and desires are put ahead of the needs of the relationship. It may even have consequences in the government as special interest groups pursue their individual interests, sometimes at the expense of the nation. In this context, the shift from community to individual exemplifies a shift from the general to the particular. People define themselves as members of the various interest groups, political parties, action organizations, rather than as United States citizens.[5]

P. J. O'Rourke carries on with the "individual" theme from a slightly different perspective:

> "A conservative believes in the sanctity of the individual. That we are individuals unique, disparate and willful -- is something we understand instinctively from an early age. Virtue is famously lonesome. Also vice, ..."
>
> "To say that we all are individual ... is simply a measurement. Individuals are the units we come in, and the individual is the wellspring of conservatism. The purpose of conservative politics is to defend the liberty of the individual, and—lest individualism run riot—insist upon individual responsibility."[6]

Changing political trends are making personal attributes more important because lives of public figures are subject to extreme scrutiny to determine their character, morality and behavior. On May 20, 1994, political consultant William Schneider told the American Association of Political Consultants that we are in the midst of a populist trend in politics in the United States. He said the voters are concerned with personalities, not party or ideology. Therefore, campaigns are devoted to destroying the opposing candidate on a personal basis.

Different kinds of pressures on individuals are emerging also. In his book "Agents of Influence," Pat Choate talks about the sale of influence in Washington. He claims that the Japanese have greater influence over the United States than the Soviet Union ever had (excluding the threat of nuclear war, of course). Japanese influence is important in the real world of economic conflict because the American and Japanese economies are the two largest in the world. The relationship demonstrates a certain American self-deception that we need to make concessions to save a relationship, and the ability of a foreign nation to exploit that characteristic as a weakness. Choate doesn't blame Japan. The problem is in American structural corruption (the sale of influence), and when combined with ignorance about the situation on the part of the American citizen, the United States is at a disadvantage.

There is a potential personnel security threat from automation which has, in a sense, lead to the creation of individuals who are technological haves and have-nots. One group of workers has knowledge, skills, and abilities to work with new technologies, but a large group of others is unprepared to cope with new demands. The latter group may take action out of frustration or disappointment. The former group might use its knowledge to engage in sophisticated criminal activity.

A symposium on computer crime at PERSEREC, held on October 25 and 26, 1993,[7] highlighted some of the issues that affect individual reliability and personnel security. Computer crime may well be the result of the development of automated information systems technology in combination with the changing attitudes of organizations which use the technology, and changes in the social behavior and moral

values of the individuals who have custody of the machinery and their contents. Persons with access to computers become criminals when they exploit the weaknesses of an organization (and its leadership) for any number of reasons: personal gain, revenge, prestige among peers, to prove their superiority through satisfaction of ego driven desires (man over machine), or because they disregard the responsibilities of their stewardship and don't believe anyone else cares.

The computer is both a target, when it is a repository of information that can be converted into money, power, or some other advantage, and the means of its own exploitation when it serves as an extension of an intelligent operator's capabilities. The computer may become the compliant partner of the trusted operator in illicit as well as legitimate activity. The law of unintended consequences can be applied when advancements in technology make it possible for someone to quickly, silently, and surreptitiously commit crimes that are most difficult to prevent and detect. The most significant problem comes from the interface between the human and the machine.

A major current failing is that our ability to create eclipses our ability to control. Technically skilled personnel create with innovation to challenge the ability of the systems and technology at their disposal, to be at the leading edge, and to obtain material rewards. Creativity produces revenue while control often restricts progress, inhibits competition, and reduces gain. In the commercial world, it is often a matter of protection versus profit. In the military and intelligence world, the amount of control imposed makes the difference between operational success and limited, delayed, or canceled operations. Officials responsible for control of systems, operations, information, often do stifle or suppress creativity. Creativity and innovation disturb their comfort zones and require them to work harder without the prospects of material rewards that come to those whose genius expands the envelope. A culture change that matches the objectives of the creator and the controller to achieve both of their goals for mutual benefit is necessary now.

In the near future, support activities and functions will be provided to government and industry organizations by specialty contractors more often than by career employees of the supported organizations. This could eliminate some of the inhibiting conflict between creator and controller as the contractor attempts to facilitate the creator's activities. However, it could be more inhibiting to the revenue-producing creator if the contractor performs strictly in accordance with an inflexible statement of work. Terms and conditions of security support contracts must be formulated in coordination with all parties affected in the customer organization.

Another significant aspect of such a situation is the amount of organizational loyalty that might be expected from sometimes temporary support personnel who have no proprietary interests in their customer's activities. Contractor personnel engaged in critical functions who are not proprietary employees may be more easily tempted to betray the interests of their customer than would full-time employees of the firm.

It is questionable whether the personnel security program can recognize or deal with the kinds of personal behavior that might allow commercial success to be placed above national interest. Today's so-called multinational or global corporation has activities and operations all over the world. Its employees are dedicated to corporate success on the one hand, and their own advancement on the other hand. Fragmented loyalties may result in unauthorized disclosure of theft of classified information or intellectual property by poorly motivated, trained, or disgruntled, unhappy employees.

To some there is even a gray area between requirements of personal behavior and the law of the land even. The conduct of personnel is questioned in terms of values and morality, even through the use of terms like "moral turpitude." Investigations seek to determine if personnel abide by the law, are good neighbors, are charitable, are good citizens. The separation of Church and State in the United States is understood. But, note the opinion of Richard John Neuhaus, Director, Institute on Religion and Public Life, delivering the 1990 - 1991 third Bradley lecture at the American Enterprise Institute on 11 December 1991:

> "A good citizen is able to give a morally compelling account of the regime of which he is a part. He is able to justify its defense against its enemies and to recommend its virtues convincingly to citizens of the next generation."

Mr. Neuhaus concludes that atheists cannot be good citizens. It is likely they would not be eligible for security clearances if he were the adjudicator.

Ray Pollari, the former Director, Counterintelligence and Investigative Programs in the Office of the Secretary of Defense, once asked me another pertinent question —

> "In a psychotic society, would a 'normal' person be regarded as too unreliable to have a clearance?"

Yes, there is doubt that the personnel security program has identified those predictors, those factors, that lead to the right questions and employ the proper techniques that will identify actual or potential traitors. Many future events can be forecast on the basis of knowledge of the world, which is based on individual experience. In personnel security, investigations produce individual histories which serve as the basis for judgement—the adjudicative files, those inanimate manifestations of flesh and blood that cross the adjudicator's desk each day and represent custodians and protectors of information, the treasure of the twentieth century. That information is most vulnerable in its most sublime form: In the human mind. It is in the memory of those represented by those adjudicative files. Each decision based on those files relates to the care, custody and control of national security information and potentially affects the balance of the world.

What happens when an adjudicator makes a mistake in judgement? The spy is long remembered. Little attention is paid when the adjudicator's decision is correct. In most cases, the decision's accuracy is never known.

CURRENT AND FUTURE ISSUES

The predication for personnel security in the 21st century will be the same as it has been and is today, but there will be different requirements. Personnel will require access to a great variety of new, developing technologies and their applications to military operations, contracting, intelligence, space and underseas exploration, as well as new and different yet unknown missions and activities of government organizations. There will be a continued need for protection of valuable assets and information, some by traditional classification, but others through more generic designations. There will likely be legislation passed to better protect vast amounts of intellectual property produced in the United States as the Congress and its constituents recognize that United States industry is disadvantaged in the world market. That legislation will restrict access to some information except to those with a need to know but, more importantly, it will provide the means to take legal action against those with access who violate their trust. It will be realized more fully in the 21st century that the national interest includes economic security and more personnel will require some kind of adjudication for access to that kind of information. It is quite likely that legislation will codify the so-called information security programs of the United States, resulting in a statutory basis for the protection of most of the nation's information of value.

The definition of personnel security for the next century must include the factor of reliability as an equal to that of trustworthiness. Personnel security must be addressed on a multi-dimensional basis that includes ascertaining the responsibility of the prospective employee; consideration of the environment in which employees live and work; cognizance of the culture in which they grew up and in which they now function; the nature, degree and extent of political influences on the employees' actions; and, the nature of the organizations in which they function.

In the context of personnel security, "employee" will refer to members of the military services, civilian employees of the government and its contractors, those with security clearances and those without. There will be fewer distinctions among cleared and uncleared personnel when it comes to accomplishing the tasks of resource protection, safeguarding physical assets, and securing intellectual property, all of which are fundamental to the security of this nation as it moves toward and into the next century.

A concept of security grounded in a national philosophy that includes practical and realistic requirements recognizing the interdependence of all contributing disciplines must be formulated to insure the national interest. Standards for the physical protection of assets; standards for the protection of information, and standards for personnel security must be developed together and consider all surrounding facts and circumstances that will have an impact on their implementation.

The Stilwell Commission nearly succeeded in establishing such a conceptually based program, and a National Industrial Security Program (NISP) plan for the future in which integrated baselines were proposed was approved by the President. The bureaucracy failed to bring either of these plans to full maturity in implementation. In these processes, the instincts of institutional self-preservation are ever-present and strong.

To manage conditions of tomorrow, personnel security officials face new challenges. U.S. military forces must deal with activities in the future that include those described by U.S. Army Operations Manual 100-5 as "Operations Other Than War." The military will be concerned with humanitarian activities, peace-keeping, illegal immigration, drug trafficking, terrorism, resource protection, crime, and as Ralph Peters puts it, "a military's reason for being is to do its nation's dirty work."[8] It is necessary to look no further than Haiti to find U.S. military personnel acting in the roles of police officers, civil affairs functionaries, plumbers, electricians, sanitary engineers, and medicine men.

The "National Military Strategy" issued by the Joint Chiefs of Staff on March 8, 1995, reflects this Administration's goals of promoting democracy and free markets abroad as well as military involvement in peacekeeping and humanitarian activities. The term used for these other military tasks is "peacetime engagement." The primary reason for the military's existence is to deter war and attacks on the United States, and, if deterrence fails, to defend the nation and defeat any enemy. The national military strategy continues to support this premise. Peacekeeping, humanitarian, and other changing roles and missions are secondary uses for forces that are bought and paid for, equipped and trained to defend this nation.

Such different military missions require an examination of the background and characteristics of the engaged personnel to include not only eligibility for access to classified information as required, but their responsibility, their mental and emotional stability, their flexibility, their ability to exercise judgement and make rapid decisions, and, generally, their abilities to deal with a psychotic society.

In these new and different circumstances, the traditional ways to determine the eligibility of our personnel for access to classified information, or to assess their reliability for assignment to some unique and different kinds of duties are not adequate. They have not been adequate for some time. For example, some years ago, foreign civilians demonstrated at a base outside the United States against U.S. nuclear weapons allegedly stored at that location. U.S. military police personnel were forbidden to cross the base perimeter, so their positions were just inside a flimsy fence which did not prevent the demonstrators from spitting on their uniforms and their bodies and assaulting them verbally. It must have been most difficult for those military policemen to keep from reacting physically to the taunting abuse. One had to be very proud of the restraint that those personnel exhibited. My curiosity as to what had prepared them for such an event found no answers except that of military discipline.

That event was like many others in foreign countries as well as at home that occurred during those days of nuclear protests and are occurring now as the military engages in prosecution of new missions. Reliability programs had prepared some of the personnel for life in missile silos, or nuclear submarines, or as members of air crews, but their managers hardly perceived a need to ensure that those personnel on the front lines meeting the public might require some of the same training. Indeed, in questioning whether the traditional ways of doing business are appropriate, one must wonder what the scope of the efforts must be in the future.

Different kinds of pressures began to affect U.S. military personnel in Vietnam. For example, as discouraging news stories continued, General Westmoreland attributed the sizable number of negative accounts to "the fault of unthinking soldiers who either acted improperly on camera or made disparaging remarks."[9] It could be concluded that a soldier under the daily pressure of Vietnam combat could not be blamed for speaking in frustration to news personnel.

In the past, personnel whose reliability in situations of extreme risk was essential have been part of a narrow population in selected environments. A "True Temper" conclusion is that existing programs are inadequate to provide assurance that their populations will perform as required or expected.[10] The Personnel Reliability Programs are often administered perfunctorily and do not instill confidence in their assurances. They do not meet the requirements of today's world in which U.S. personnel must carry out missions in risky environments in which multiple, simultaneous threats are extant to include sabotage, espionage, terrorism, theft, and armed conflict. The population of concern extends beyond conventional forces, or Special Forces, to astronauts, submarine crews, personnel in remote locations, peacekeepers, and many more. The future will demand even more emphatically that these personnel be reliable, responsible, and eligible for access to classified information frequently.

There are correlations among the processes that determine suitability for a job or position, reliability in carrying out the duties of that job, and eligibility for access to classified information. It may be easier to describe the differences among the three, but in doing so it is impossible not to also identify the similarities. In its simplest form, suitability means that someone is appropriate for a particular function. Determination of suitability is based on factors of experience: In today's world, some of those factors are an individual's experience with use of alcohol, or drugs; sexual behavior; financial responsibility; criminal activity; or indicators that a person is inclined to break rules which is often a basis for a deduction that a person is not responsible. Irresponsibility, of course, is a potentially disqualifying factor in determining eligibility for access to classified information, as well as a significant factor in assessing someone's suitability and reliability. Responsibility becomes a common criterion in assessing someone for duties, jobs, and access to classified information.

Reliability, ascribed to something or someone you can depend on, is not merely a subjective designation. While suitability is transitory, a guess, an attempt to forecast what

someone's performance will be on the basis of past experience, reliability is a matter of performance against standards. Reliability can be tested. It is a constant. Reliability can be determined by monitoring, evaluating and analyzing someone's performance. Selecting someone potentially reliable, of course, requires some of the same forecasting ability as selecting someone who is suitable for a particular job or who is eligible for access to classified information. The distinctions among the criteria or selection on the basis of reliability, suitability and eligibility are blurred. They are all applicable to personal performance in which security is an integral part. In the future, personnel selection and access adjudication processes will be integrated in response to increasing requirements for more reliable personnel to have access to more critical information of various kinds. Integration of these processes will require, as PERSEREC is aware already, the development of new and better evaluation criteria, testing methods, and techniques for screening and monitoring of personnel.

Factors that have an impact on behavior other than those pertinent to protection of sensitive or classified information come into play when a military squad leader must run a gauntlet of angry local gunmen in a foreign village, or deal with a mob of criminals in a small, island nation. These sorts of future activities will require that our personnel be prepared for different challenges, and their qualifications must include all the factors of reliability, responsibility, and suitability that lead to success in assignments requiring loyalty, integrity and discretion.

These probable future situations are not without peril. The new and changing circumstances of our military personnel already create unrest among them and their dependents. Uncertain military missions, often without much chance of victory in the traditional sense and with diminished resources, contribute to low morale. "It doesn't take a rocket scientist to figure out that military people are frightened, insecure, unhappy--and that's the people who are staying in," said Daniel Nelson, director of international studies at Old Dominion University and a military consultant. "The human level stresses, the money, careers--it's tearing at people."[11]

In terms of the general population, many economists, sociologists, and politicians are reporting evidence of a world increasingly made up of "haves" and "have nots" in which those better trained and educated will improve their lot; others will see their fortunes diminish. Such circumstances can produce disgruntled employees or applicants, who might seek retribution and resort to criminal actions to improve their circumstances. The technological "haves" and "have nots" referred to earlier form a microcosm of this general population.

The threat of national programs such as Medicare, Medicaid, and Social Security going bankrupt or being cut puts a heavier load of responsibility on the individual. Despite that fact, according to a CNN - Gallup Poll reported on CNN Headline News, April 21, 1995, more than two-thirds of Americans over the age of 30 have not yet begun saving for retirement. And, Olivia Mellon, a psychotherapist in Washington, D.C., says "about 75% of Americans have some kind of problem dealing with money. Just thinking

about money makes many people worry about not having it." Worry may incite some to violate their trust and sell government or corporate secrets for personal gain.

Government or corporate downsizing with accompanying resource restrictions contribute to employee or former employee disgruntlement. According to new research, "... the factor most predictive of violent behavior is not a history of violence or mental illness or drug abuse; it's being laid off from a job."[12] It was reported by the Department of Justice in 1994 that nearly one million people experience some sort of workplace violence every year. It will be a future security requirement to take preventative measures in the hiring process to screen out potentially violent employees.

Unhappiness among employees or former employees can lead them to seek alternative means of support. A growing list of organizations to include militia that promote conspiracy theories might well appeal to some. Beliefs that the United Nations plans to conquer the United States, or that FEMA will head up an interim government, might appeal to someone unemployed without prospects for an income in the near future and who wants to get even for real or imagined transgressions against him.

A global economy continues to mature. That simply means increased trade in goods and services and international flow of money, people, and information. Personnel find themselves in strange and different environments subject to pressures For which many are not prepared.

The espionage cases of the past few years have created a preoccupation among government officials with protection of classified information to the detriment of efforts to protect proprietary information, intellectual property, and other sensitive data that has jeopardized the economic security of our nation and, quite frankly, removed jobs from America. The new world in which we have entered, requires a broader view of the needs to control all information significant to the welfare of the United States.

"Information Warfare," or INFOWAR, is the in vogue terminology that is partly a description of an old, continuing national, corporate and individual struggle for possession and control of, or access to information that provides competitive advantages or enables actions favorable to one of the parties.

According to *Time* magazine (August 12, 1995, p. 40), Admiral William Owens, Vice Chairman, Joint Chiefs of Staff, in referring to INFOWAR, said, "this is America's gift to warfare." With all due respect to Admiral Owens, America is not the single contributor of this capability to the world, nor can it be assumed that the United States holds all the advantageous positions in this war. In fact, the military's recognition of the applications and opportunities of cyber techniques may well illustrate that INFOWAR refines the way modern warfare has shifted toward civilian targets. The United States presents many targets for adversaries throughout the rest of the world.

INFOWAR threats to air traffic control systems, telephone systems, stock exchanges, banking and financial networks, as well as theft and manipulation of various privileged data are not new. They are sabotage, espionage, and malicious damage in new clothes. They are elements of economic warfare that can jeopardize national stability and security through infrastructure damage. The fact that they are being recognized more readily and can be employed more dramatically requires that the methods and means of acquisition, custody, control, protection, transmission, and sharing of information be examined in modern and future contexts.

THE FUTURE

"Americans have been accustomed in the past to think of national security too largely in purely military terms. Today, it is obvious that valid national strategy must embrace all our natural resources of every kind--human, material, industrial, scientific, political, and spiritual. The Armed Forces are simply the cutting edge--a deterrent to hostile action in ordinary time but when used in war, a last and desperate resort. Military policy and preparation are vital, but they are only a part of national security policy as a whole, which, if it is to succeed, must continuously integrate political objectives, military plans, economic strength, and civilian organization into a comprehensive and carefully formulated national policy and purpose."[13]

That definition of national security in 1949 by Louis Smith is applicable today and will be tomorrow as well. Concern over finding the right policies to guide personnel security in the 21st Century is based on the fact that only sporadically over the years has the United States integrated all of the factors delineated by Smith into a strategy to protect the national interest. There is another opportunity to do so in the next 100 years. Even so, it is an uncertain possibility that policies and procedures can be established and tested over a reasonable period of time which will produce a reasonable personnel security process applicable to all persons in every situation where access is required to information that must be protected to promote the national interest.

Too often, too much effort is invested in trying to provide lasting solutions to transitory problems. The pace of change in the next century will preclude the issuance of hard and fast rules designed for application to a stable target population. Rather, guidelines must be designed that will allow cognizant officials to use judgement in determining whether individuals may or may not have access in specific circumstances. Central repositories of accessible data will enable adjudications to be made instantly by the official who is best able to determine need to know. Each individual certified to potentially need access will have been subjected to an eligibility determination which will reside both in data base and in the individual's possession in the form of a smart card, perhaps. It is quite possible also to imagine access achieved at a particular location simply by passing that card through an electronic scanner which coordinates with the data base and approves or rejects the cardholder's access on the spot. Clearance and access not touched by human hands will be the rule.

The future policy base must allow for rapid modification, revocation if not feasible, adjustment if necessary, continuous reexamination, and application when practical. Such a policy attitude will be necessary to deal with the uncertainties of different circumstances. It rejects the practice of basing every decision on history and tradition in favor of innovation and resourcefulness. It will ensure the flexibility needed to support events and function in environments yet to be created. The 21st Century frontier in personnel security will be characterized by a return to judgement on the part of every participant in the program.

The paths of the public and private sectors will cross more often. Classified information as we now know it will disappear eventually. In its place will be a body of data that includes all information necessary to ensure the national interest—political, military, economic, to include intellectual property. Information requiring safeguarding either by statute or executive order will be specified and administered in accordance with the provisions of a National Information Protection Program.

Reaching this state will not be easy. History has demonstrated that professionals in their chosen fields of interest and endeavor are notorious for being victims of their own enthusiasms and prejudices and for considering that their own theories are the most authoritative. There is no reason to believe that proponents of the status quo will succumb without a fight.

Senator Daniel Patrick Moynihan has quoted from Philosopher Thomas S. Kuhn's book, *The Structure of Scientific Revolutions*, in which Kuhn used the word *paradigm* to describe the model of the way the world works that makes sense to people at the time--and that causes a good deal of trouble when a competing view comes along. Kuhn's argument is that theories give meaning to facts, rather than, in any simple sense, arising out of them. "The essential point is that for people wedded to a particular paradigm, everything inside that paradigm makes sense. Everything outside sounds, well, crazy." As we approach the 21st Century, some people are going to go through a painful divorce from their present program partner because personnel security in the 21st Century will not be dealt with successfully using the 20th Century paradigm.[14]

Individual responsibility and accountability will be more important, partly because of the increasingly sophisticated technological abilities to gather, process and transmit large amounts of information at high speeds. And, partly because more U.S. citizens will be responsible for protecting that information and other valuable assets at remote locations throughout the world.

The requirement for individual responsibility in the next century forces the recollection that the Athenian Democracy was founded on two cardinal principles: an absolute acceptance of the laws (including what we would call the constitution) ... and the belief that everyone in the society governed by those laws had an equal right and almost an equal duty to administer them.[15] The more things change, the more they remain the same, perhaps.

Personnel security guidelines for the next century certainly will include some standards that will form the baseline for eligibility and entrance into the eligibility data base. The standards will adjust to the prevailing morality. People will continue to have some affinity for all the things that personnel security standards now attempt to control - sex, pornography, violence, controlled substances, and uncontrolled spending. The challenge will be just as now, to determine the significance of the candidate's activities in terms of requirements of the candidate's position.

Whatever standards are established cannot be illusory. They cannot be so unrealistic as to be unattainable. Although, perhaps they have been in the past because Justice Douglas reportedly commented that the standards established in the Government's loyalty program were such that even the President couldn't meet them. But, the standards must be commensurate with what they are designed to help protect everything of value in the possession of those declared trustworthy.

Risk management is a current buzz phrase. If it is to be applied to personnel security, those involved in administration of the program will need to understand, as the insurance industry and the Department of Defense have for many years, that the key word in the phrase is *risk*. In setting standards, there must be a clear determination made as to what the government is willing to lose. There is a point beyond which expenditure of resources to protect something is not feasible. The burden of risk falls on the standard because threat is never constant, and vulnerabilities are hardly ever the same among those in the eligible population, and certainly not in all of the environments throughout the world in which personnel must operate.

Personnel security standards are also dependent somewhat on the value of that which is to be protected. Value, in turn, is somewhat dependent on the needs of those who require the valuable commodity, or those by whom it is coveted. So, personnel security standards must be devised on the basis of what must be protected and who must protect it, as well as where it will be protected.

Risk management must be adventurous and permit investment in personnel who have characteristics that indicate a high tolerance for risk. Some method of "risk and return" analysis should be devised to reach the clear understanding of the risk government is willing to take to achieve its objectives. The objectives are the "return" in the equation and are measurable: Secure operations; contract performance free of compromise; an espionage-free work force; employees who are stable in tough situations, reliable despite temptation, loyal to their employer and their nation. Risk is more difficult to quantify, although it can be evaluated to some extent by fluctuation of results. The degree of fluctuation can be measured by a statistic known as standard deviation. The greater the standard deviation, the greater the risk.

Such an analysis translates into correlations:

Conservative standards—lower risk
Moderate standards—moderate risk
Liberal standards—higher risk

These correlations also enable decentralized management and reliance on the judgement of officials on the scene, leaving the central data base authority to attempt dispassionate application of standards.

A great beginning has been made in understanding some of the fundamental questions and principles underlying the issues of personnel security, reliability, and suitability. There are still many things unknown about the relative reliability of our techniques and sources. Still unknown also is why some people are still willing to risk their freedom, and ours, by committing espionage merely for material gain. For some, there is and no doubt will continue to be a certain reconciliation of risk, however misguided, between civil liberties and the perception that those liberties allow the commission of espionage.

Aldrich Ames, for example, "...calmly attributed his ability to undertake what prosecutors described as "a crime that caused people to die" to mentality that was shaped long before he began his work for the Soviets." He claimed that his dual existence as an open State Department employee and a private one as a CIA operative forced him to "compartment" his mind. Despite having taken loyalty oaths, he sold sensitive secrets because: "I tend to put some of these things in separate boxes, and compartment feelings and thoughts."[16]

Others who have committed espionage have separated their professional activities from their treason and rationalized such behavior as insignificant because they did their job very well. Such rationalizations might become more prevalent in the future, particularly in the realm of economic espionage where it is easier to believe that illicit sale of protected information is not harmful to the national security. Nicholas Leeson brought Barings Bank of London to its knees through deceptive actions, if not fraud, and is a current example of one who abdicated fiduciary responsibility, partly through the failure of his employer to recognize the opportunities of its employee and to take preventive measures through supervision, at least.

In drawing a caricature of a future participant in personnel security programs, Tim McVeigh must be part of the background at least. The following excepts from *The Washington Post* of July 2, 1995, are pertinent:

> "In deeply disturbing ways, he is a prototype of his generation. He lived the divorce revolution, age 10, when his parents split for that increasingly familiar reason: They were just too different. He was an underachiever in

high school, uninterested in college. He hit the job market in the mid - 1980's as it ran out of room for young men with blue collar skills.

"He worked dead-end jobs, voiced fears of going nowhere, tried a well trod escape route—the Army—but bailed out as the military downsized with the fall of communism. Like millions in his generation, he ended up back home as an adult, a man sleeping in a boy's room headed exactly where he'd feared: nowhere.

"He was indistinguishable from everyone else ... Even the problems in his life ... were average.

"Someone who has talked to him since the bombing said, "There's nothing alarming about him—nothing. He's respectful of his elders, he's polite. When he expresses political views, for most of what he says, Rush Limbaugh is scarier. That's what's incredibly frightening. If he is what he appears to be, there must be other people out there like him. You look at him and you think: This isn't the end of something, this is the beginning of something."

"For the most part, any aberrations in Tim McVeigh's life were hidden under an exterior so bland as to be nondescript."[17]

A 20th Century personnel security program has no more chance of identifying a Tim McVeigh than someone who is committing espionage.

"A kid from the heart of America who feels society has let him down can be very dangerous if he has underlying emotional quirks," said Charles Bahn, a forensic psychologist from John Jay College of Criminal Justice in New York who studies the psyche of terrorists. "In urban America, gangs fill this void. In the Midwest, it's cults, the macho gun world, militia, belonging to fringe groups."

Those who seek acceptance and support from fringe groups are likely to be among the technologically disadvantaged as well as one of the general "have-nots," but may be members of the military, employees of government contractors, workers with access to assets of value and protected information. Some of them will be participants in the personnel security programs of the future as candidates for access, as accessed personnel, as debriefed personnel who continue to recall that to which they had access.

John Dilulio describes another future problem:

"Because of the demographic cohort of teenage men—half a million more coming into the population by the year 2000--we are confronting a new criminal class and yet another crime wave that we are virtually powerless to stop."[18]

These teenage men are potential military members and government employees some of whom will be candidates for positions of trust and responsibility.

It is apparent that the program of the future must be administered at the level where most is known about those requiring access. That means the program will depend on leadership.

Program administrators and managers must motivate citizens to accept responsibility for their actions. Those in leadership roles must understand that they are dependent on personnel accessed in the program. For successful results, all program participants, those who administer and manage, and those who must follow the guidelines, must cooperate. Personnel management must be integrated with personnel security administration. And, they both must be integrated with technology because every subject of the personnel security program can be converted to an adversary by a modem or an airplane. Integration of management functions should prevent situations like that of Aldrich Ames who, after receiving a poor rating in the Office of the Deputy Director for Operations at CIA, was assigned to the counterintelligence center--a reward for weakness.

The program must focus on customer needs through a doctrine of customer dynamics. Everyone must be made part of the process. The engineer must understand why personnel security is important. Program managers, CEOs and security personnel must speak the same language to ensure that they are building a common culture. The customers of the program must be dealt with personally. Affected personnel should be involved in the formulation of policies, standards and procedures.

A fundamental requirement for the next century will be to create employees who are loyal to the organization and the program. They must understand how they contribute to the success of the program. The "insider" must be trustworthy, and individuals with malicious intent must be prevented from becoming insiders. Robert Louis Stevenson allegedly claimed that "everyone lives by selling something." The personnel security program must be sold to its participants, not imposed on them. Perhaps the most important part of managing risk is engaging program participants as partners in the process.

Teaching the accessed population what is right and convincing them that it is useful is part of security education. Awareness is the capital of the security process. It involves understanding the criteria for asset protection; the needs for protection; options available; individual responsibilities; and, the consequences of the failure to behave properly.

Security awareness, education, and training programs of the future must deal with the matter of continuing evaluation of personnel through training and education of supervisors at all levels concerning the security dimensions of their responsibilities. The supervisor must notify personnel what is expected of them from a security standpoint as well as their expectations of technical performance. Security must become a performance

standard clearly communicated from supervisor to employee. Supervisors and personnel officials must understand how to train, monitor, and take action in cases where security standards are not met by employees. In this integration of security and personnel management, it will not be possible for managers to avoid facing the training issue. Training funds must be provided to develop the integrity of staff members along with their skills to increase productivity, improve service, utilize them fully and in these ways, reduce costs.

Michigan State University Professor David Carter identified and reported to PERSEREC some benchmark criteria that serve as critical elements in the prevention of espionage and theft of corporate secrets. Many of the benchmarks apply to asset protection generally and to the reliability and responsibility of personnel. Some of them are:

Selection. This refers to the recruitment and employment of personnel who have been screened for their substantive knowledge, competence, loyalty, psychological stability, and social stability. While selection is not fail-safe, it is an important beginning.

Training. Beyond giving a new employee the substantive knowledge and procedures related to his/her new position, training can provide insights and threats related to security. Training should also include in-service sessions to present new information and reinforce security procedures.

Supervision. Supervisors must be vigilant to account for the behavior--and particularly changes in behavior--of personnel under their supervision. An alert supervisor may both identify when an employee has committed a security violation as well as perceive signs which could be the precursor of such violations if intervention does not occur.

Accountability. Whereas surveillance refers to property or information control, accountability refers to control of individuals. Ensuring personnel are following procedures, performing efficiently and effectively, and adhering to organizational values will contribute greatly to continued personnel integrity.

Positive Work Environment. Having a good work environment, being supportive of one's place of work, and having a feeling of worth in the organization--a sense of ownership--will increase the employee's obligation and loyalty to the organization. As these factors increase, the probability of espionage by employees will decrease.

Realistic Threat of Discipline for Wrong Doing. Given the nature of information (and property) which is at issue in light of national security and economic intelligence, employees must also recognize that if they commit a security violation there is a realistic threat that they will be both identified and disciplined. Punishment must be swift and sure if it is going to have any significant preventive effect.

Positive Rewards. Balancing the realistic threat of discipline is reinforcement of positive work and contributions to the organization. Supervisors and managers must provide a positive environment for work performed well by providing rewards, awards, and commendations. The spirit of cooperation is what should be engendered within the organization, not competition.

Reinforcement of Ethics and Values. A statement of organizational values, reinforcement of ethical standards, and the obligations of professionalism must be engendered in all employees. At the least, all employees should subscribe to the most basic of all ethics--"Do no harm." This sense of moral obligation can be an important security precaution.

There are no simple answers to determination of eligibility for access to classified information or to the reliability of our personnel in any sort of assignment. The problems are complex; the solutions are complex, but these benchmarks will assist next century officials to manage the conditions that exist where they must administer the program.

Prevention of espionage goes beyond security practices and programming. It involves the entire management and human resources system of an organization in order to create organizational loyalty and diminish the potential for one to commit espionage. The government personnel security program objective of determining eligibility for access to classified information must change in the 21st Century. It will, as previously indicated, include programs that determine reliability and responsibility for duty performance and protection of things and information of value.

The centerpiece, or activity of greatest emphasis will shift from the background investigation to a concept of fairly broad surveillance of individual characteristics and identity.

For many years, I have believed that determinations of suitability, reliability, and eligibility for access to classified information might be possible by forensic means. Advances in brain wave phenomenology and genetic mapping may well provide future opportunities that haven't yet been imagined. Perhaps the day will come when the prospective employee or applicant can walk into a facility and his or her aura will transmit the necessary indications that a suitable, reliable, eligible individual has arrived.

Recently, *Time* magazine reported that magnetic resonance imaging (MRI) and positron-emission tomography (PET) are letting scientists watch a thought take place, see the red glow of fear erupt, and note the telltale firing of neurons as a long-buried memory is reconstructed. Johns Hopkins has launched the Zanvyl Krieger Mind/Brain Institute and Harvard has created the Mind/Brain/Behavior Institute. Dr. Rodolfo Llinas, New York University Medical School, using a device called the magneto-encephalograph, which indirectly measures electric currents within the brain, has measured the electrical response to external stimuli.[19]

It's only a matter of time.

In the meantime, can future behavior be predicted? In the absolute sense, perhaps not. In the sense of making a forecast, a statement about what one thinks will happen, maybe. To assist in transition from traditional means of forecasting to more sophisticated future techniques, some sort of inquiry into the backgrounds of candidates for positions of trust will be conducted.

The transition investigation will include an applicant's submission of background data by electronic means. The central data bank will maintain the information both for security and employment purposes unless the candidate or applicant objects. The information will be kept for security reasons as long as necessary. There will be controversy over how much of what kind of information must be submitted in order to determine basic qualifications for access and duty. There are those who object to providing information concerning criminal behavior; others object to offering details concerning foreign travel; some are reluctant to provide information about personal wealth or family affairs. A most important submission will be that which claims birth or citizenship, two items that must be independently verified. It seems quite likely that the issue of sexual preference will disappear as a matter of concern in personnel security in the future.

Subjects of investigations will be informed about what is to be done with data submitted and collected. If information is collected for storage in government archives without analysis or application, the subject should have the option to submit information or withhold the data. If the information is to be used in confidence to determine indications of perfidy or patriotism, then such use will be demonstrated through relevance to the individual's status--cleared, accessed, or denied for specified reasons.

File checks will be accomplished through automatic coordination of data bases to determine public records of misbehavior, or the absence thereof, as well as credit history and contents of appropriate financial records. Verification of birth and identity comprise the fundamental factor in the investigation. Individual financial records such as income tax filings, if any, will become conveniently accessible and may be part of the initial submission of data by the applicant.

A personal interview of the applicant will follow appropriate file checks and record reviews. The initial interview will include verification of submitted data, resolution of discrepancies, evaluation of detected anomalies, and information will be provided to the subject concerning his or her future responsibilities.

If the inquiry is favorable to this point, the data should be entered into the central data bank and placed on a chip in a smart card which will also contain the subject's personal, medical, military, education and law enforcement history. The card indicating eligibility for access to protected information, will be carried by the subject. If unfavorable information is developed, necessary investigation will be conducted to

resolve issues. It is expected that the measurable result of initial transition background investigations will be a relatively low rate of applicant rejection. Just as now, deterrent value of the investigation will be impossible to measure.

Departments and agencies using investigations for access determinations and employment suitability will have different measurable results in terms of restricted or unrestricted employment and access to data.

Resources saved by automating and simplifying the initial background investigation can be used subsequently at random intervals to determine the stewardship of the individual as a custodian of classified information and as a performing employee. Continuing evaluation of security performance will include periodic screening for positions of greater responsibility; physical and mental fitness evaluations; integrated security education and training that supports career enhancing assignments; and, personal interviews to identify problems. The objective of an interview will be to identify and fix problems stemming from financial irresponsibility, interpersonal conflicts, stress, personal relationship issues, and anything that affects the employee's stability. Specialty techniques such as use of the polygraph will be used only in attempts to resolve issues when no other solution is available. This will track with the increasing concerns for fairness to the individual and full benefit of the employing organization. Other techniques like psychological tests or other instruments that might produce evidence of mental fitness, stability, reliability, dependability, adaptability, and general suitability for enduring the responsibilities of difficult assignments or protection of valuable assets may be used as necessary to meet the standards of the individual's current or prospective assignment.

The smart card carried by the individual, an Individual Data Card (IDC), will be presented and read electronically at the individual's employing activity whenever the person needs access to data necessary to perform assigned tasks. Eligibility will be automatically confirmed by the central data base as the card is read locally wherever the employee needs access. The automated process will also record where the individual had access and to what information.

Personnel security, personnel management, and technology will be integrated throughout the process. For example, multi-level security (MLS) will be an information management tool that protects sensitive information of all genders in processing, handling and transmission modes. The privilege of an individual to gain access to classified or unclassified protected information controlled by MLS will be based on "need-to-know." This security technology tool will be part of a principal security management process that prevents system users from obtaining access above their assigned levels. As access decisions will be virtually automatic and at the local level, the needs of both the organization and the individual are met. The individual's IDC, of course, in coordination with MLS, determines access.

Arrests of an eligible individual or other transgressions affecting his or her eligibility will be entered on the IDC at the time of occurrence. A continuous history of the eligible person will be maintained eliminating the need for frequent human intervention in that part of the process. Continuing evaluation of an individual's professional and security performance will be accomplished by both human and automatic means. Such a program should provide greater assurance of an employee's loyalty and productivity reducing an organization's security risk and improving its economic gain.

A SUPPLEMENTAL NOTE

Risk management is the business of minimizing risks.

Despite our illusions to the contrary, the risk in personnel security comes from things we can't control: Our own personnel with access to classified information; and, an adversary. The risks are in the form of the vulnerabilities of the individual and the probability of that individual's betrayal, and the threat of the adversary.

Our burden is to recognize, understand, and attempt to quantify the risk so something can be done to reduce the likelihood of damage if an adversary's actions and an individual's vulnerabilities interact.

There are two kinds of risk assessment. One is emotional and one is practical. Asbestos removal from public buildings is an example of emotional response to a possible threat. According to *Smithsonian* magazine (November 1995), one person a year dies from ingesting a toothpick and that is a higher death rate than what results from asbestos exposure.

There is a tendency toward emotionalism when dealing with risks to national security also. But, we need to be practical. There is a dichotomy here, isn't there? We must be practical, but we must take risks.

How much risk can we take in the name of "national security?" We attempt to answer that when we assign values to the things we believe worthy of protection. We believe some parts of the national security require more protection than other parts. We investigate people needing access on the same basis.

So we determine our actions directed toward minimizing risk on the basis of arbitrary assignments of value to things, and arbitrary determinations of investigative scope applied universally to every candidate for access to things of value. Overlaying all of this is a belief that there is someone else who wants what we are protecting--a threatening adversary.

We have a system of ambiguities the exercise of which results in ambiguous pay-offs.

There is cause and effect at work here somewhere but the actuarial tables are incomplete. I believe there is one binding conclusion that we must follow: Don't apply limited resources to negligible risks.

SUMMARY

In the 21st Century, more individuals will be collaborating on diverse ventures in different areas of the world. Individual trustworthiness will be a credential. The personnel security programs must concentrate on supporting individual inclinations toward trustworthiness. The programs must take advantage of change and enable high levels of innovation and creativity. The programs must emphasize value and quality through establishment of education, training, and research programs that will support all program participants. The programs must be flexible; formulated in context with organizational missions; integrated with personnel management programs; and convey requirements to participants effectively and quickly. The programs must accommodate changing circumstances by engaging participants in devising policies and procedures, and the programs must be administered at the lowest possible level of bureaucracy.

Environmental, societal, cultural, political, economic, and military trends and their affects on personal behavior will demand that the programs keep pace with the world. This is the concept that will guide the United States toward a system that creates a single view of national security requirements.

Personnel security is more important now than ever and will continue to increase in importance in the next century. The ability to grant or deny access to information is, and will be, a primary consideration. Information control is the critical function; it can be accomplished by technical means but only through human implementation.

Those who control the information domains through the mechanisms of advanced technology will form an information priesthood. Their ministrations will govern the congregation. They who control the systems and those granted communion through access to the products of the systems must all be loyal, honest, reliable, and responsible believers.

ENDNOTES

1. See Keeping The Nation's Secrets: A Report to the Secretary of Defense by the Commission to Review DOD Security Policies and Practices, November 18, 1985, named in honor of its Chairman, the late General Richard G. Stilwell, USA (Retired)

2. See Maynard C. Anderson, A Prudent Approach to Industrial Security: The National Industrial Security Program, March 1992

3. See Redefining Security: A Report to The Secretary of Defense and The Director of Central Intelligence, by the Joint Security Commission, February 28, 1994

4. See Target Revitalization for Espionage in American Industry: New Directions For the Coming Decade, a Grant Report to the Defense Personnel Security Research Center, September 1993, by Dr. David L. Carter, Michigan State University

5. Clint Schnekloth, "Falling Into Orbit," A work in progress, Luther College, Decorah, Iowa, May 1995

6. P.J. O'Rourke, "Why I Believe What I Believe, " Rolling Stone Magazine, July 13-27, 1995. P.53

7. See Computer Crime: A Peopleware Problem, Proceedings of a Conference held October 25-26, 1993, at the Defense Personnel Security Research Center, Edited by Dr. Theodore R. Sarbin

8. Ralph Peters, PARAMETERS, Vol. XXV #2, Summer 1995, P.7

9. William M. Hammond, PUBLIC AFFAIRS: The Military and the Media, 1962-1986, Washington: Center of Military History, 1988. P.322

10. Richard Nelson, TRUE TEMPER Project Symposium Lectures, Armed Forces Radiobiology Research Institute, Bethesda, MD, December 3-4,1993

11. David Wood, Newhouse News Service, "Malaise in the Ranks," The Raleigh News and Observer, August 28, 1994, P. 17A.

12. Time, August 29, 1994, P.21

13. Louis Smith, American Democracy and Military Power: A Study of Civil Control of the Military Power in the United States, Chicago: The University of Chicago Press, 1951, P.319

14. Daniel Patrick Moynihan, "Our Stupid But Permanent CIA." The Washington Post, April 29, 1994, P. C3

15. W.G. Forrest, The Emergence of Greek Democracy, McGraw Hill. New York, 1966, P.221

16. The Washington Post, April 29, 1994, P.1

17. Dale Russakoff, and Serge F. Kovaleski, "An Ordinary Boy's Rage," The Washington Post, July 2, 1995

18. John J. Dilulio, Jr., and Donald Kettl, "Fine Print: The Contract With America, Revolution, and the Administrative Realities of American Federalism: A Monograph, The Brookings Institution, Washington, 1995

19. Michael D. Lemonick, "Glimpses of the Mind," Time. July 17. 1995.

SEYMOUR HERSH

Mr. Hersh's early career as a journalist included being a police reporter in Chicago, a UPI correspondent in Pierre, SD, and an AP correspondent in Chicago and Washington. He was with the *New York Times* from 1972 to 1979, both in Washington and New York and from 1983 until 1986 he was national correspondent for the *Atlantic Monthly.*

Mr. Hersh's books include *Chemical and Biological Warfare: America's Hidden Arsenal* (1968); *Cover-Up: The Army's Secret Investigation of the Massacre of My Lai* (1972); *The Price of Power: Kissinger in the Nixon White House* (1983); *The Target is Destroyed: What Really Happened to Flight 007 and What America Knew About It* (1986); and *The Sampson Option: Israel's Nuclear Arsenal and America's Foreign Policy* (1991). In 1970 he won the Pulitzer prize for international reporting. Other awards are for stories on B-52 bombing in Cambodia (1973), for stories on domestic CIA spying (1974), Drew Pearson prize for stories on CIA involvement in Chile, and for articles on CIA involvement in Libya (1981).

SECURITY: ANOTHER PERSPECTIVE

Seymour Hersh

Because of technical difficulties in recording this talk, we offer a brief synopsis of the presentation, with apologies for the loss of flavor and suspense created by Mr. Hersh's telling of the tale.

In the context of leaks of sensitive information, Hersh discussed with the audience how journalists work. He took us "on a little tour of the ethics of the profession" that might relate to security. He wanted the audience to put themselves in the place of a young reporter, to learn what reporters do in the field and what kind of techniques they use. He told us the story of how he broke the Calley case during the Vietnam era. He had been working as a freelance writer, producing articles and books, several of which concerned the military. He was young, recently married, didn't have a regular job, and was hungry for "fame, fortune and glory."

He learned casually by way of a friend's phone call that there was a big case brewing involving the prosecution by the Army of a lieutenant accused of murdering 75 Vietnamese civilians. Hersh admits that he was tempted, not just by the story itself, but by the thought that it would surely lead to glory, even a Pullitzer if he was lucky. So he began "horsing around with it," "making investigations, running around, calling, checking, going through every file, every base" looking for the case. Through diligent effort, he eventually learned of the base where the case was being prosectued and discovered the name of the accused, Lt. Calley and, equally important, the name of his defending counsel in Salt Lake City.

A flight to Salt Lake City found Hersh in the office of Calley's lawyer. The lawyer brought out the charge sheets and read to Hersh the charges being brought against Calley. Then he was called from the office. He left the file open on the desk.

What is a young, hungry seeker of fame and fortune to do? That was the moral dilemma with which Hersh confronted the *Vision 2021* audience in 1996. If we had been in his situation, what would we have done? This led to lively discussion among the audience. Then Hersh upped the moral ante: What if the lawyer had placed the file in a drawer and not locked the drawer? What would we have done in his position? What if he had left the file in a safe and not locked the safe? More discussion from the audience on the moral gradations posed.

Hersh's moral position was clear: Taking the file would be theft, a morally unacceptable choice. Hersh told how he obtained the information without compromising his moral standards. On the lawyer's return he engaged the lawyer in a 15-minute conversation, at the same time surreptitiously copying in his notebook all the relevant information on the exposed charge sheet, reading the charge sheet upside down. Hersh

also told of informal ways of gathering information that was supposed to be protected. Working the Pentagon, he became friendly with military officers, joined in poker games. Not infrequently, an officer would reveal sensitive information, the motive being ego-enhancement.

The moral of the story for security professionals? If journalists who are diligent and resourceful can obtain sensitive information, then men and women with intent to spy can make use of the same kinds of information-gathering techniques.

HARRY LETAW, JR.

Dr. Letaw is Chairman of the Board of Directors, President and CEO of Essex Corporation in Columbia, MD. Essex provides Human Centered Systems Engineering, opto-electronic image and signal processors, multimedia training materials including simulators, and a variety of related engineering, support and manufacturing services. Dr. Letaw has served in senior management and technical positions with Raytheon Company, Martin Marietta Corporation and Bunker Ramo Corporation.

WHAT *CAN* WE PROTECT IN 2021?

Harry Letaw, Jr.

To know what we can protect in the Year 2021, we must understand strategies for information containment to be used in the future. This daunting challenge demands that we somehow experience and appreciate the immense changes that will take place over the next 25 years. Their impact on society, institutions, technology and patterns of thought will surely be profound. For example, only 25 years ago, the ABC, CBS and NBC networks were reported to have transmitted the programs of that day "almost exclusively" in color.[1] Today, a cornucopia of worldwide program resources transmitted in a rainbow of video has nearly completely erased memories of sitcoms viewed in monochrome.

In 1971, the personal computer revolution was still a decade in the future. Many will recall our fascination with the power of the four-function electronic calculators of the time. And, 25 years ago, we had few benchmarks to estimate the consequences of the Federal Communications Commission's important decision not to regulate computer data communications.[2] We were unable to peer a quarter century into the future and grasp the heavy influence of this decision in securing the vast social, economic and military benefits that have lately arisen from the information communications revolution.

Since making predictions is difficult, perhaps we can finesse the process with one giant, imaginary leap into the Year 2021. We will arrive there as participants in a seminar tasked to analyze the currents of thought that led to the information containment procedures then practiced by the military-industrial complex. From that vantage point, with hindsight to guide our speculation, we will project today's trends as best we can 25 years into the future. You will decide the degree to which this methodology is successful.

Before we journey into the dynamic, creative whirlpool of technology and commerce of the Year 2021, let us take stock of some of the problems that we will encounter as we shift mental gears to become a 21st Century audience. Our "speaker from the future" will assume that we are familiar with such things as optronic components called Sclen-Ops(TM) and the materiel movement service, RoboNet(SM). He will know that many of us are employed by "Paradigm Four," an institution that is completely unknown to us as we stand solidly grounded in the 20th Century. Paradigm Four has not yet been organized and Sclen-Ops(TM) and RoboNet(SM) are surely not to be found in this century. Now, here is our 21st Century speaker.

A long season of productive change was set in motion by social and technical forces put into play during the last half of the tumultuous 20th Century. The sudden end of the major superpower confrontation was a pivotal event, capped by the unexpected collapse of the Soviet Union. That astonishing outcome followed four decades of vigorous, touch-and-go competition. This result was believed by many to demonstrate, at

least in part, that closed societies could not, in the long run, compete successfully against open ones.

Open societies share the benefits of technology under a system of laws that protect intellectual property interests. Closed societies hamstring themselves with draconian internal security controls long since constrained within open societies. Progress in open societies was accelerated by the growth of information networks enabling seamless exchanges of technical and other information. The open private sector rose to levels of economic and intellectual vitality that could not be matched by more controlled, would-be competitors.

As the last quarter of the 20th Century unfolded, the seeds of change were visible to any who wished to see them. The United States of America, for practical purposes, possessed a monopoly on many of the most highly valued technologies. The U.S. faced a genuinely powerful military challenge; however, the technology that it brought to bear in the encounter was intrinsically more flexible and far more broadly useful than that of its principal adversary. A thicket of silicon-based smart weapons offset forests of artillery and herds of armored vehicles. While heavy steel forgings have an obvious place in commerce, sensors, high-speed computers and wideband communications find much larger markets in products of higher added value.

The Free World economy was underpinned by easily accessed stores of knowledge. Means of production were widely distributed. The United States and its closest trading partners built strong relationships that led not only to growing military power, but also to burgeoning economies in which billions of people participated. Entrepreneurism at the very high end of technology was stimulated by the ready availability of powerful components, such as lasers and computer chips, that in some respects enabled a "basement shop" to compete with major development laboratories.

Progress was not uniform. Late in the 20th Century, a *Scientific American* magazine staff study pointed out that in Sub-Saharan Africa, a slow and feeble connection from a personal computer to the Internet cost $65,000 per year, a stupendous sum at the time. Even more amazing, the average waiting time for installation of a primitive wireline telephone in most of the region was nine years. The coastal Africa fiberoptic ring was completed at the end of the century.[3] Communications in Africa soon became relatively cheap and readily available, vastly simulating continental economic and technical activity.

Similar network expansions brought distant sites close together. A key milestone of progress was the emergence of cellular satellite systems. For the first time, they allowed anyone, anywhere on earth to speak directly to anyone else, wherever located, with autonomous, hand-held telephones. The web of wired and wireless networks expanded in response to seemingly limitless human need to exchange ideas and data. The ease and low cost of communicating inevitably led to distributed transnational

engineering, scientific and mathematics projects, many involving small, highly entrepreneurial enterprises.

Profound changes in "information ownership" arose from these forces. This was recognized before the turn of the century by John P. White, then Chairman of the U.S. Commission on Roles and Missions of the Armed Forces, who wrote, "...(S)cientific, technical and organizational innovations will increasingly come from outside DoD's sphere of influence. Reduced budgets will not allow DoD to underwrite the breadth and depth of research that was possible in the past."[4] Note that "DoD" signifies the U.S. Department of Defense, an exceedingly large military organization of the time. It is the approximate functional equivalent of today's Paradigm Four, or "PF" to most of us.

Such acceptance of openness foreshadowed contributions by information networks to key advances in technology during the first decades of the 21st Century. Small and medium sized groups with great technical and industrial competence almost literally bubbled up everywhere in the world. Technical information was developed, disseminated and applied with great speed. The impact of the robust information infrastructure upon society and government continued unabated into the present year.

National military projects became increasingly dependent on commercial and foreign assets, a dependence that extended well beyond raw materials, components and economic offset programs. Entire technologies became inextricably private and transnational in character, as exemplified by the Russia-U.S. supersonic transport aircraft program.

In the second decade of this century, the invention and commercialization of the stunningly powerful Sclen-Ops(TM) optronic components brilliantly integrated optics and electronics. They performed mathematical operations at speeds vastly greater than ever before achieved. Nearly all high-speed, state-of-the-art information systems became completely dependent upon that technology. This invention was made by the Egypt-Israel-Palestine (EGISPAL) consortium. It had the effect of creating a virtual monopoly that the consortium was able to maintain for nearly a decade. The result was comparable to the non-exclusive, but tight lock held by Japan on small appliance manufacturing in the Seventies and Eighties of the last century.

Sclen-Ops(TM) were far more valuable, and certainly more useful, than gold. They were prime movers in rendering "hands-on" merchandise transport systems obsolete because of their vulnerability to pilferage. A rudimentary automated courier system, derived from earlier work in "Smart Highways" and "Free Airways," was soon introduced. It evolved into the rarely penetrated RoboNet(SM) transfer service upon which the entire world depends today for fast, safe, economical materiel movement.

Speed in completing product development was seen to be essential for commercial success. Similarly, military programs increasingly valued speed in bringing new systems to deployment. It became clear that the more people there are in charge of any project, the more likely it is to take longer than it should. The more vigorously the

state-of-the-art is pushed, the greater the development effort, and the more time that elapses between system definition and deployment. Applying any constraints that are only marginally related to product functionality also proportionately slows the deployment cycle.[5]

Growing awareness of these simple concepts triggered major military procurement reform initiatives. Whenever possible, non-developmental items are used. Military specifications and standards are not applied to them. They are off-the-shelf articles that will perform the desired functions, perhaps requiring specialized packaging to resist the rigors of military environmental conditions. In all respects, including industrial security, the objective is to simplify and accelerate acquisition.

In 1995, then Deputy Undersecretary of DoD for Acquisition Reform, Colleen Preston, presciently wrote, "Maintaining the edge by keeping our technology secret is no longer a viable strategy. The key today is to be the first to integrate the technology already out there. Whoever succeeds will maintain the superior force."[6] As she predicted, critical portions of projects were declassified to facilitate participation by transnational teams. Many such teams are unwilling to deal with classification and other constraints, strongly committed to retaining intellectual property and manufacturing rights, and are, in fact, "the only game in town."

Over the next 25 years, military acquisition processes were systematically simplified. Expensive custom designs were largely replaced by economical "racked and stacked" commercial off-the-shelf, "COTS," products. Many systems and upgrades were designed and fielded with leadtimes of a few months. Even though certain information was "compromised" by transnational openness, as Preston forecasted, timeliness and ease of acquisition operated to preserve tactical advantage.

Classification was limited increasingly to key, critically sensitive information elements such as algorithms and combat frequencies. These items fall well within the spirit of the Espionage Act in any era. Use of RoboNet(SM) allowed sensitive information, stored in a few easily secured repositories, to be dispatched immediately, as needed.

Throughout history, the greatest threat to information containment has been the disloyal servant with legitimate access to sensitive information. As our predecessors noted, "With enough money, a safe can be cracked from the inside." The practice of limiting the number of classified items and locations in which they are stored greatly reduces both the cost of protection and the number of persons requiring access. The question remains: How does one assure continued reliability of trusted persons?

People who work together form small groups bound by common interests, no matter how large an entity their employer may be. Three-quarters of a century ago, after World War II, such mutual interests led to the creation of Quality Circles, first in Japan. Quality Circles are a mechanism that allows small groups of workers, perhaps ten or fewer, to focus some time and effort toward identifying and overcoming barriers to

quality production. They gained momentum as workers recognized that their livelihood depended directly upon the quality of products shipped. There is an immense literature on small group process and the techniques of establishing and supporting Quality Circles.[7,8,9]

In 1980, Donald Dewar wrote, "A Quality Circle is a way of capturing the creative and innovative power that lies within the work force."[7] The underlying rationale is to benefit from the desire and capacity of people to participate in managing their own work. This aspect of human nature also applies to functions other than Quality. For example, maintenance personnel in certain petrochemical plants have banded together in Safety Circles because of their dependence upon one another for on-the-job survival. In this way, they learn, motivate one another and guard against a catastrophic event.

Security Circles were first created in smaller enterprises to counter threats to their existence posed by industrial espionage. People whose jobs depended upon intellectual property devised means to assure information containment. Coming from the bench, rather than from above, based on rice-bowl economics, rather than *force majeure*, Security Circles became positive bulwarks against leakage of both proprietary and classified information. As their functional power was increasingly appreciated, older rule-based modalities imposed from above began to disappear because they were seen to be no longer cost-effective.

Management assists in the formation of a Security Circle, but does not lead it. Management provides information about threats and vulnerabilities, helps in the development of guidelines and fosters the growth of the Security Circle movement in the institution or company. Members of a Security Circle have a clear understanding of what is and what is not "sensitive." They are given time to organize and to hold brief periodic meetings within their own Circle and with members of other Circles in the plant. The process is aimed at developing a frame of mind focused upon protecting precisely the information that protects jobs. This is an excellent definition of sensitivity.

Let us now turn back the clock and return from the world of 2021 with a somewhat better understanding of options available to us. The forces acting today to change our views on information containment are very powerful. As we have seen, DoD Management has validated some of the key trends. Are the inferences that we have drawn from these trends extreme? Understated? About right? Of course, it is beyond our powers to provide that answer. Nevertheless, our community is obliged to set a course toward the future. Either we plan for the future, or it will be thrust upon us.

Security Circles do not exist today, but people with common interests share common purposes. Among those they activate are the few members of any design team who fully appreciate and understand the critical design details that are often deeply buried within systems. Security Circles might be found to have additional merit in containing costs and stimulating participative cooperation.

Security Circles harness powerful human drives. To an increasing extent, people at all levels in technology-based industry realize that specialized knowledge is their meal ticket. Everyone understands that compromise of information, proprietary or national security in nature, takes bread from our mouths. Security Circles can become a valuable tool to deal with the complex, dynamic tasks of information containment in the 21st Century.

Let us admit that we are unlikely ever to be fully capable of thwarting the treacherous actions of spies or zealots, no matter how many compartments we erect. We must recognize that inflicting "Ames' Revenge" on honest, hard-working people with blizzards of never-to-be-read financial statements, hyped-up procedures, and ever more elegant electric couches does not deal with gut issues. Instead, we must attend to the well-being of the people entrusted to us, take personal interest in their morale, and ensure their professional growth. Steps taken to build job satisfaction and mutual trust are low-cost initiatives that contribute immensely to effective security in a productive environment.

Today, the importance of classification is waning under the pressures of the need for simplicity and economy. Unclassified proprietary commercial products deliver performance and economies of scale not otherwise attainable. Networked transnational technical teams increasingly drive the state of the art. In the world of nodes, nets and rapid response acquisition, strategies of information containment are changing rapidly.

Let us recognize, in the spirit of this gathering, that the obsessive secrecy of the Cold War has no role in the 21st Century. Effective strategies are available and should be used to protect core assets. It is reasonable to project, however, that achieving and maintaining state-of-the-art performance within closed environments is all but unaffordable today and will surely become impossible in the future.

REFERENCES

[1] *Britannica Book of the Year 1971* (1971). (p. 703c). Chicago: William Benton.

[2] *Ibid.* (p. 701c).

[3] Gibbs, W.W. (1995, August). Lost Science in the Third World. *Scientific American*, 92-99.

[4] White, J.P. (1995, Issue 2). How to get to the Future. *Defense 95*, 11-17.

[5] Smith, P.G. and Reinertsen, D.G. (1991). *Developing Products in Half the Time*. (296 pp.) New York: Van Nostrand Reinhold.

[6] Preston, C. (1995,Issue 2). Re-engineering DoD's Procurement System. *Defense 95*, 18-22.

[7] Dewar, D.L. (1980). *The Quality Circle Guide to Participative Management*. (414 pp.) Englewood Cliffs: Prentice-Hall, Inc.

[8] Crocker, O.L., Sik Leung Chiu, J., and Charney, C. (1984). *Quality Circles: A Guide to Participation and Productivity*. (294 pp.) New York: Facts on File, Inc.

[9] Barra, R. (1989). *Putting Quality Circles to Work*. (200 pp.) New York McGraw-Hill Book Company.

ETHEL THEIS

Since August 1989 Dr. Theis has served as the Information Security Oversight Office's (ISOO) Associate Director. In this position, Dr. Theis participates in the development and implementation of policies and procedures on classifying, safeguarding and declassifying national security information. Dr. Theis was heavily involved in the administration's efforts to revise the classification system, and in the development and subsequent implementation of new presidential policies in this area.

ETHEL THEIS, Discussant, SESSION III

I am delighted to be here. Yesterday's panelists not only informed but challenged us with the many new ideas they put forth. Today's panelists promise to be just as challenging and informative.

As a discussant, I have two major objectives in mind. The first is that I want to keep my remarks short. My purpose is to give the audience the opportunity to have a reasonable amount of time to ask questions of the panelists. Secondly, I want to provide you with a summary of some of the major points made by each of the panelists on this morning's program. As I discuss these points, you will notice, as I did during my review of Maynard Anderson's and Harry Letaw's papers, some areas of convergence in thought and action between them concerning personnel and information security today and in 2021.

During my review I also noticed some areas of convergence on personnel and information security issues between Harry's and Maynard's views and those expressed by some of the panelists featured on yesterday's program. I won't tell you what these areas are, but I would like you to think about them during my discussion. I find that this convergence on some of the key issues in personnel and information security among individuals from different backgrounds and interests--academia, government, industry, the Congress--bodes well for bringing about needed change. Such convergence could prove a powerful vehicle for bringing about change.

My original intention was to start with Maynard's and Harry's papers and then turn to Seymour Hersh's presentation. Unfortunately, Mr. Hersh could not stay for the discussion segment. I was tempted to ask him before he left whether he was manipulating us when he told us what good guys journalists really are, and what a strong sense of ethics they have. But he is such an entertaining speaker that, after a while, I didn't care if I was being manipulated because I was having so much fun listening.

I reviewed Maynard's paper last night, all 61 pages of it. There was so much to absorb. So I apologize to Maynard if I do not do full justice to his effort. I don't think that quality and quantity always go together. In the case of Maynard's paper, however, I have to admit that they do. He has done an excellent and thorough job of combining lessons from the past in order to offer prescriptions for the future. Most importantly, his prescriptions are "do-able."

Harry's eight-page paper, on the other hand, reminded me of my response when some people call me small. My response is: Good things *sometimes* come in small packages. Harry's paper is *definitely* a good thing in a small package. His paper gave me pause for reflection, particularly his concept of security circles.

The importance of Maynard's historical approach is that it provides a clearer perspective of the weaknesses of prior, or current for that matter, personnel systems and points a direction for future action. Equally important is that his proposals for future action are grounded in the realities of "what can be done," translated as what would be accepted and implemented by the bureaucracy. We are all familiar with sound policy issuances full of promise, which failed because of lack of or poor implementation.

During his research Maynard found one common theme implicit in the criticisms of the various groups that have analyzed the personnel security program over the years. That common theme is that in personnel security, the process has become more important than the results. That emphasis on process has led to the neglect of other areas. This neglect is particularly harmful with regard to security education and training for individuals having access to classified information. But, as Maynard points out, to be effective such training must go beyond the mechanics of teaching procedures. It *must* seek to change individual's attitudes by having security awareness become an accepted norm of behavior. This new behavior would create an environment in which an individual's willingness to accept responsibility for protecting information would be an integral part of job performance.

As to the future, Maynard rightly notes that current and new technologies make more pressing the need to devote energies and time to change patterns of behavior. This involves commitment to inculcate in individuals a respect for the protection of classified information. In short, I would say that what Maynard proposes in this area is the development of a "culture of protection" among individuals who hold security clearances.

Another important point that Maynard makes in his paper, and one that is shared by many political scientists, concerns 1950s notions of national security. Looking at national security primarily in military terms places any nation-state at a disadvantage versus other nation-states. The primacy of the military component of national security has given way to a broader conception encompassing politics, economics, scientific and, even, environmental affairs. As we head into the future, it is more than likely that the military aspect of national security will become subordinated to these other issues.

But as Maynard points out, "paradigms" or "world views" are not easily replaced. Although Kuhn was offering the concept of paradigm shift to explain changes in the way we do science, his concept is just as applicable to personnel or information security. When people, and we all do this to some extent, have vested interests in the way things are done, change is not easy to achieve.

Harry's paper presents us with a view of what the world of 2021 may look like to personnel and information security people. I found his futuristic approach quite refreshing. His concept of the security world of 2021 would certainly present a "new paradigm."

Harry sees the future as one in which the application of sophisticated technology has helped eliminate or modify many of the personnel and information security problems we face today. In this world, technology has helped shift the emphasis from secrecy to openness. Also, in this world economics plays a key role as speed in completing product development is seen as essential for commercial success. These developments are accompanied by a much closer relationship between government and industry, as well as by a growing cooperation and interdependence between domestic and international groups. In such a world, technical information is developed and disseminated quickly within and across national boundaries.

As Harry indicates, in this new world less classified information means lower information safeguarding costs, and lower costs for personnel security clearances. But as he points out, even in this new world the question that remains is, "How does one assure continued reliability of trusted persons." In seeking an answer to this question he suggests the creation of Security Circles, derived from the idea of quality circles, as a possible solution.

These security circles could provide an answer to the problem because they would be accompanied by a change of focus on how to deal with individuals. The security circles concept envisions an environment where job satisfaction would be the rule rather than the exception, and managers would take more of an interest in employees' morale and personal growth. This might commit [my word] the individual to become a part of the system rather than an outsider with no stake in the proper working of the system.

SESSION IV

PETER SADERHOLM

Mr. Saderholm joined the CIA in 1963 where he worked until 1977 with the Office of Imagery Analysis or its predecessors. During this period he had a 2-year rotational tour with the National Photographic Interpretation Center and for 2 years was in charge of a branch of photo interpreters in Thailand. In November 1977 he began a tour in the Office of the Comptroller. In October 1981 he was assigned the position of Executive Officer for the Office of East Asian Analysis. He became a Division Chief in the Office of Central Reference in 1985. Three years later he was reassigned as Deputy Chief of Collection Requirements and Evaluation Staff in the Directorate of Intelligence, becoming Chief of this Staff in June 1992. In August 1994 he was selected for a new position as Director, Security Policy Board Staff.

SECURITY: MAKING IT WORK THROUGH RECIPROCITY

Peter Saderholm*

Mr. Saderholm noted that he is a civil engineer by trade. He has been a career employee of the CIA since 1963, serving in a number of capacities with that agency. He has been the Security Policy Board Staff's Director since its founding in September 1994.

Prior to his present position, Saderholm had always been a consumer of security services; he now wears a national-level mantle as a producer of such services. In that vein, he presented an historical view of the security community: a community in a high state of confusion, with little or no reciprocity among departments and agencies, and little or no focus on risk management. He related that confusion to a large number of agencies taking a variety of actions in the name of security without much coordination. That, in turn, led departments and agencies away from any degree of comfort as far as accepting security decisions made by others. In other words, there was no trust of the existing security processes or apparatuses between and among departments and agencies. Saderholm stated that he firmly believed that the ultimate, long-term success or failure of the Security Policy Board would hinge to a large measure on its ability to foster and sustain reciprocity for security decisions made within the security community.

Saderholm expressed his views of the nature of security in the year 2021. He foresees:

- Departments and agencies maintaining their separate legal authorities to carry out their assigned missions, yet having a common security goal, and operating with flexible, jointly produced, universally accepted security policies. To achieve that posture, though, people who are expected to accept those policies need to be brought into the policymaking process, a hallmark of the Security Policy Board strategy for giving the nation effective security at a price it can afford.

- All security policies will be based on analysis. A clear understanding of why we must take certain safeguarding actions in the interests of securing valued assets.

- A national perspective of concern for safeguarding valued assets that are translated into classification guides. We need to have a clear, government articulation of what is important to the security of the nation, and that articulation must be embodied in publicly available statements.

---

* This is a precis of Mr. Saderholm's presentation written by SPB staff.

- A renewal, if possible, of the need-to-know principle. We need to get away from rigid control mechanisms built on security processes and, instead, abide by a process that allows people access to information only if they need it to do their assigned jobs.

- Security procedures for discrete levels of information access which will be the same for government and industry. Government and industry need to protect like information and interests under the same set of rules.

Saderholm concluded his presentation by echoing Maynard Anderson's earlier call for a "return to judgment." He said that for security to be successful in the 21st century, it needs to focus on the positive, not the negative. It must shift away from a perception of being the "bad cop," i.e., recommending sanctions against people who violate security rules, and instead focus on being the "good cop," convincing the government and industry populations at large that security policies are based on sound, rational analysis, merit respect and appropriate individual practice, and are implemented through fair and equitable processes. He said it was incumbent on the security community to serve as a mentor to the population it serves by ensuring that individuals are able to discern what needs to be protected from that which does not.

Finally, Saderholm urged everyone to think about these new security processes, and to think about the criticality of ensuring our nation's security as an acceptable and honorable way of life.

KENNETH GEIDE

Mr. Geide has had a long career in the FBI. He has extensive experience in counterintelligence and is Chief of the Economic Espionage Unit at the FBI. He is intimately involved in the effort to protect our information infrastructure and is taking an active role in computer crimes as they relate to counterintelligence issues.

ECONOMIC ESPIONAGE: LOOKING AHEAD

Kenneth Geide

NOTE: We were unable to capture Mr. Geide's talk on tape. The following is an abstract taken from PERSEREC and Policy Board staffers' notes.

Geide began his talk by discussing the present environment where, with the end of the Cold War, economic security and national security have become almost synonymous. This presents special challenges in this new environment, especially in corporate America. Corporations are being robbed to an unprecedented degree of their innovative technologies, know-how, and other intellectual property. We are all victims, public and private alike, of these new attacks and the new methods used to perpetrate them. And the problem reaches across all domains--government, private sector, law enforcement, counterintelligence and foreign intelligence.

The FBI has set up an economic counterintelligence unit that is distilling information from FBI investigations and making this information available to security managers in the public and private sectors. Within the past 1 1/2 years there has been a 100% increase in the number of economic espionage investigations managed by the FBI. Some 800 cases of alleged economic espionage are currently being investigated, involving 23 different countries. FBI's responsibility is to counter such attacks.

Geide pointed to a central problem in protecting intellectual property. Statutes are written to punish persons who steal tangible property. However, the life blood of a corporation is the ideas, plans, intellectual property. For example, if a desktop computer valued at $5,000 or more is stolen and transported in interstate commerce, a federal law can be invoked to investigate the crime and to prosecute the offender. But if the same person were to download intellectual property that resides in the computer, worth far more than $5,000, no federal law could be invoked to apprehend or prosecute. The Congress is considering bills that would protect intellectual property.*

Geide believes that economic espionage by foreign countries will continue to increase, the targets being the same--intellectual property and other proprietary economic information. There is a concern that in the future more and more economic espionage will involve computers and automated information systems and networking. For this reason, the FBI has created a computer investigations and threat assessment center, bringing together FBI criminal, investigative and CI elements. This center will eventually provide threat and vulnerability information, both classified and unclassified, to the public and private sectors.

** The Economic Espionage Act of 1996 was signed in October 1996 by President Clinton. This act federalizes the theft of trade secrets. If stolen information is proprietary, was properly protected by the victimized company, and had potential value to the company, its theft is now a federal offense. Punishments include 15 years and up to $10 million fine, which is returned to the victimized company.*

DAN SMITH

For more than 21 years Dr. Smith has been involved in the evaluation and design of safeguards and security (S&S) systems for the private nuclear industry and for the government-sponsored nuclear materials production and nuclear weapons production industries.

Since 1991 Dr. Smith has been Program Manager of the S&S Technology Development Program within the Department of Energy's Office of Safeguards and Security. He leads a team of project managers who manage and oversee developmental projects in material control and accounting, physical security, information/computer security, personnel security, protective force technologies, and integrated S&S systems. He has initiated a series of interagency security technology exchange meetings, involving individual agencies with the federal security community and representatives from the counter-terrorism, counter-drug, intelligence and military special operations communities. He and his staff have also established direct technology exchanges between DOE, other agencies, and other nations; presented or participated in program reviews, briefings and demonstrations of S&S technology with other agencies and private industries; and chaired or represented DOE in several interagency organizations.

The following paper was co-authored by Carl Piechowski, Electrical Engineer, Technology Development Program, Office of Safeguards and Security, U.S. Department of Energy.

FUTURE SECURITY/ ANTI-TERRORISM TECHNOLOGIES: CURRENT PERSPECTIVES

G. Dan Smith and Carl Piechowski

INTRODUCTION

The U.S. Department of Energy (DOE) is responsible for conducting and managing a large number of activities that directly support national and international security. For more than 30 years, the Office of Safeguards and Security's Technology Development Program (TDP) has been responsible for initiating, advancing and applying state-of-the-art technologies to protect nuclear weapons materials, facilities and information. More specifically, major portions of the TDP's challenging, diverse, and evolving concerns include:

- Developing the means for the physical protection and control of Departmental personnel, equipment, laboratories, production facilities, nuclear materials, and other such property.
- Providing capabilities to precisely identify and measure (weapons grade) nuclear materials.
- Maintaining very detailed accountability of the status of DOE's nuclear materials.
- Preventing the spread of weapons of mass destruction (i.e., nuclear weapons.)
- Ensuring that many different types of data, with divergent levels of sensitivity, remain accurate and appropriately available to its owners and users while prohibiting access by unauthorized individuals.

As DOE's nuclear weapons complex converts from its production mode of the past to one of downsizing, modernization, limited operations and more appropriate alignment with its current mission, many factors add complexity to maintaining the desired level of security. Among the most pervasive of those constraints are:

- Major environmental cleanup is occurring at our facilities, often requiring uncleared workers to operate in sensitive processing facilities, and also requiring large quantities of additional nuclear materials to be stored, accounted for and protected.
-
- Ever present forces from shrinking budgets are causing DOE to rely more heavily on technological solutions (instead of personnel) to maintain its level of security operations.

- Large numbers of decommissioned weapons are being accepted by DOE from the Department of Defense for dismantlement and storage. Likewise, DOE has assumed stewardship of significant amounts of nuclear material (shipped and stored here) from the Former Soviet Union (FSU).

- As the absolute size of the DOE complex continues to diminish in response to its changing missions, the heightened potential that disgruntled current or former employees will engage in malicious activities exists.

BACKGROUND

COORDINATION: As may be readily imagined, there exists a significant amount of overlap in the types of security related technologies which various Federal Agencies and the U.S. Military require to protect their assets and operations. In order to facilitate efficient sharing of successful developments and to prevent inappropriate parallel or duplicative efforts, the TDP regularly participates in inter-organizational technology exchanges and coordinating groups. The specific character of those activities (which include various combinations of government and industry representation) differs from group to group, reflecting the focus of that group's objectives.

CUSTOMERS: The following list represents the types of end users supported by the TDP.

Direct customers include DOE:
- National Laboratories
- Facilities
- Sites
- Field Offices
- Headquarters

Indirect Customers include:
- U.S. Military
- Other Federal Agencies
- State and Local Governments

Law Enforcement
U.S. Private Industry

GOALS OF THIS PRESENTATION: Although it is virtually impossible for any individual or organization to accurately forecast the environment that the United States Citizens and their Government will be facing several years from now, the intention of this paper is to raise the audience's level of awareness regarding the current, emerging and foreseeable problems associated with protecting the key assets of the DOE and the public it serves.

GENERAL PERSPECTIVE: By now, it is no longer news that the Cold War between the United States and the Soviet Union is not being waged as it was for so many years. However, the world has changed dramatically many times and in many ways throughout recent history. As stated earlier, we cannot predict the future with any certainty. What we can count on though, is that changes will continue to occur. Regardless of what the nature of those changes might be, the U.S. will almost certainly remain a primary target for domestically and internationally motivated acts of terrorism. As a subset of that statement, emerging forms of "techno-terrorism" may exploit the U.S. dependency on automated information systems (information warfare), the escalating capability of foreign nations to radically compete with the U.S. economy (economic warfare), or may resort to such heinous methods as nuclear, chemical or biologically based attacks (weapons of mass destruction).

In the world of applied technologies, there will also continue to be a "leap-frog" effect whereby the providers of technological security solutions must expect that those solutions will be defeated by new attack methods requiring different solutions to be developed. This scenario is especially true in the world of information technology which continues to experience the effects of rapid growth, leading to the need for accelerated and insightful developments in the areas of security policies, technologies and applications.

The terrorist specific threats to our facilities, our operations and our assets as a whole may come from traditional sources. However, there are many non-traditional and unexpected adversaries whose existence must be considered when planning for the protection of the assets for which we are responsible. There are several recent examples that highlight how diverse those threats can be. The party responsible for bombing the Oklahoma City federal building was initially suspected by some to be an Islamic extremist (or group). However, it now appears likely that the attack was initiated wholly from within the borders of the United States.

The Aum Shinri Kyo religious sect that is is allegedly responsible for the gas attack on Tokyo's public subway system is another prime example of a non-traditional adversary that built and applied a capability to inflict mass suffering, death and terror. A final (and less publicized) example refers to an individual who displayed the potential (if not the outright intent) to commit another serious attack using a biological agent. In early 1995, a well and tank inspector, working for a laboratory in central Ohio, illegally obtained $300 worth of Yersinia Pestis (the bacteria that causes Bubonic Plague) by misrepresenting himself to the organization that distributes the bacteria. Although no people were infected with the bacteria obtained (the inspector was arrested), it still demonstrates the unpredictable and very real nature of the terrorist threats that we are beginning to experience within our own country.

As those examples, and the bombing of the World Trade Center building in New York demonstrate, the targets of terrorism's destructive activity are not limited in terms of geographic or national boundaries. That is why no individuals or groups responsible

for security system planning, design or implementation can feel comfortable with the status quo; but, must continuously re-examine the constraints and requirements of the environments within which they are operating.

A final example of hostile activity attributable to politically motivated aggressors involved the French Ministries of Health and Education. On December 14, 1995, many Internet users coordinated a "flooding" of certain French Government computers as a protest of that nation's nuclear testing policy. Flooding a network simply means to overload it with users and activity, thus rendering it inaccessible to its legitimate users.

Although technology in itself is not the solution to all of the problems we are facing, it can provide the tools that the security community needs to balance the costs and performance impacts being experienced by security system users in response to escalating and greatly divergent threats.

EMERGING TECHNOLOGIES

The TDP organizes its program according to three principal security categories. They are: Physical Security (including Protective Forces), Information Security (primarily Computer Security), and Material Control and Accountability. As an overview of how the TDP is dealing with some of its perceived security issues, each of these security categories will be outlined in the following sections which will provide some level of insight into the types of concerns that are being addressed by the TDP, technologies initiated by the TDP in response to those concerns, and the types of end users that will employ those technologies.

PHYSICAL SECURITY: The goals of the physical security programs at DOE include preventing unauthorized access into Departmental facilities; detecting and responding to attempts to gain unauthorized access to DOE facilities; preventing the theft or malicious destruction of any portion of those facilities, DOE owned nuclear materials or property; maintaining a relatively safe environment for the large number of people within the DOE complex, and for the American public; and protecting against activities conducted to obstruct DOE operations.

The first line of defense in the layered protection approach is to deter and prevent hostile activities. Some methods used to preclude security incidents are physical barriers, manual and electronic access control systems, and security guards. If those preliminary methods fail, further levels of protection are provided by locks, additional physical barriers, automated intrusion detection sensors, closed circuit television, and protective forces. In preparation for aggressive and potentially successful attacks against DOE assets, response capabilities include components such as integrated alarm assessments, response forces, secure communication systems and frequently exercised plans for back-up support from other agencies.

If any of DOE's critical assets are lost to an adversary, DOE response forces would engage in "hot pursuit" in attempting to locate or recover them. The participants in

such a pursuit would include DOE's Nuclear Emergency Search Team (NEST), the FBI and the DoD Special Operations Command (SOCOM).

Considering the concepts profiled above, there are many opportunities to improve the security posture of DOE in terms of effectiveness and efficiency by developing or applying emerging technologies. For example, the TDP has been developing remote and physically harmless human presence detection methods for examining large cargo, vehicles, etc., for a trojan-horse insertion of adversaries. Other instances of emerging technologies are portable security systems; explosive (and other contraband) detection portals; chemical and biological agent detection, identification and protection gear; and laser radar for use as an early warning tool to detect perimeter intrusion attempts. Using biometrics to identify people is another area of ongoing development efforts. Biometric refers to technologies that employ the concept of identifying who a specific individual is by evaluating their distinguishable and unique physical characteristics. The TDP has also developed and fielded non-lead (environmentally safe) frangible ammunition which would not be healthy for armed adversaries, but would greatly reduce collateral injuries and damage versus traditional types of ammunition.

To summarize the constraints that affect the development and use of these technologies, it is important to note that contemporary Departmental priorities include more than simply applying effective security measures. Those measures must also be designed in a manner that maximizes the safety of employees, visitors, and the public, as well as minimizing the loss of facility operating time. A number of non-lethal protection technologies have been explored and are the preferred methods to use if possible. The large number and diversity of people, materials, technologies, operations and facilities that DOE must protect adds to the difficulty of effectively protecting against all of the associated security threats.

INFORMATION SECURITY: Throughout the DOE, there exists an overwhelming amount of information in the form of electronic data. Large portions of that data are classified or sensitive unclassified. Electronically formatted data that is collected, created, processed, transmitted, stored, or disseminated by or on behalf of DOE requires graded, cost-effective protection. Ensuring its integrity, availability, and confidentiality is essential to the success of the Department's various missions. Furthermore, loss or compromise of the Department's information may place at risk the nation's competitive economic position, the environment, the national security, other U.S. Government missions, or the citizens of the United States.

A short, example list of information categories within DOE could include proprietary design data, other types of intellectual property, personnel information, nuclear weapons designs, weapons testing, commercial strategies or partnerships, energy conversion and distribution, medical research, advanced computing, materials research, and advanced manufacturing techniques. Once again, excessive damage to DOE, organizations that do business with DOE, and the U.S. public could result from the loss of that information to our adversaries. Other concerns related to the protection of DOE

information assets include maintaining the integrity of data, and preventing the potential for obstructing critical components of the U.S. infrastructure[1] that depend on automated information systems (AIS).

Information protection is largely dependent on administrative measures such as data user and owner awareness, AIS administration, etc. However, in order to mitigate the frequency and consequences of network and computer break-ins, the TDP is continuously considering new applications of technology to detect intrusions, automatically evaluate network security, and develop multi-level AIS which combine users who possess various levels of security clearances or data access privileges into a single system.

AIS are considered to be the most rapidly changing and unpredictable technology that we are facing. As hackers, software viruses, malevolent insiders, techno-terrorists and other malicious agents are rapidly advancing and automating their attack capabilities, the number and severity of attempted AIS security incidents is escalating.[2] The TDP is developing two different types of technologies to detect unauthorized attempted access or suspicious activity on DOE computer networks. One technique focuses on known attack signatures, while the other focuses on single events that may signal the steps preceding an attack on a network.

Earlier this year, the network intrusion detection tool that was developed for the TDP by one of DOE's National Laboratories was subsequently used to identify, track and arrest an international computer hacker that was suspected of breaking into U.S. military, Government, and university systems. There are two significant aspects to that activity. This was the first time a court-ordered wiretap was used on an AIS (data network). Secondly, the tool was configured to provide investigators only with recordings of the specific hacker's activities, while protecting the privacy of the thousands of other legitimate users on the same network.

The constraints that affect the development and use of computer security technologies include concerns for performance effects that such security tools place on systems; dramatically evolving rate of technological change, constantly increasing number, connectivity and sophistication of computer users; the ability for adversaries to

---

[1] Electric power grids, Telephone systems, Communication systems, Power generation facilities, etc.

[2] "... Specialized Technical Operations. This includes computer intrusions, telecommunications targeting and intercept, and private sector encryption weaknesses. These activities account for the largest portion of economic and industrial information lost by U.S. corporations." (From the *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*, published by the National Counterintelligence Center, July 1995.)

attack systems from far-away places; and the fact that AIS have both physical and virtual perimeters to protect.

MATERIAL CONTROL AND ACCOUNTABILITY (MC&A): As the title of this security discipline suggests, it has two primary objectives, controlling the location of, access to, and movement of DOE's nuclear materials; and maintaining detailed and accurate knowledge and records of the location, amount and form of DOE's nuclear materials.

Theft, smuggling and illicit marketing of weapons grade nuclear materials remains as a critical international concern. Since the DOE maintains stewardship of large amounts of such materials, those concerns are a major issue to the Department. Even though DOE is no longer producing large numbers of nuclear weapons, the return of decommissioned weapons, and the large scale decommissioning and decontamination of entire DOE facilities is resulting in new MC&A concerns due to the large quantities of additional nuclear materials that must be safeguarded.

The TDP's products are being applied internationally through the U.S. nuclear non-proliferation program, which is using DOE safeguards and security technologies and training to strengthen International Atomic Energy Agency (IAEA) safeguards. Direct laboratory to laboratory exchanges between DOE and member states of the former Soviet Union (FSU) are resulting in application of TDP developed technologies to securing FSU nuclear materials against theft or diversion.

The technologies being developed to counter both current and future threats include more accurate nuclear material detectors, nuclear material measurement instruments to account for material that was previously unmeasurable due to its chemical form or where it was located, modular vaults that can be used to temporarily store materials at sites undergoing environmental restoration, and vault and material surveillance systems that monitor the location and intrinsic properties of materials in storage (e.g., heat, weight, radiation, etc.)

Where possible, humans are being removed from direct contact with nuclear materials. For example, material measurement systems that automatically transfer their data to accounting systems, and automated vault monitoring technologies, each serve the dual purpose of reducing human exposure to dangerous environments while simultaneously aiding the protection of nuclear materials by inhibiting direct human access to them. The goals of maximum employee safety and increased protection against

"insider" threats are partially satisfied by those types of systems. Insider is the term used to identify people that have legitimate working responsibilities within the DOE complex, yet may engage in malicious activities against DOE, national security, and public health and safety[3].

SUMMARY

As the collective set of DOE missions and responsibilities continues to evolve in response to changing national and international conditions, new threats to national security are expected to arise. Furthermore, existing threats may persist in their traditional, or in significantly modified forms. Given those expectations, there is ample reason to forecast that the development and application of technological solutions to security-related problems will be a crucial part of protecting the U.S. population, as well as its commercial and Government owned physical and intellectual property. The benefits of such applications include favorable cost-benefit ratios for security system planners, designers and operators, who seek to provide protection implementations that are as effective as possible, yet financially and functionally feasible. They also include the ability to provide security solutions that can operate in environments that limit the use of expensive and frequently ineffective manual or human components. The scope of what security technology developers must provide to their customers and users will change dramatically between now and the next quarter century. However, in whatever form, application of existing and emerging technologies will remain interwoven into security solutions into the foreseeable future.

---

[3] Examples include disgruntled employees, agents working for foreign interests, and other types of malevolent individuals or groups that may emerge within DOE facilities..

LINTON WELLS II

In 26 years of naval service Mr. Wells, a 1967 graduate of the U.S. Naval Academy, served on a variety of surface ships, including command of a destroyer squadron and guided missile destroyer. In addition, he acquired a wide range of experience in operations analysis; Pacific, Indian Ocean and Middle East affairs; command, control, communications and intelligence (C3I); and special access program oversight. Prior to his present appointment in November 1993 as Deputy to the Under Secretary of Defense (Policy) for Policy Support, Mr. Wells served as Assistant to the Under Secretary of Defense (Policy). Mr. Wells has written widely on security studies in English and Japanese journals.

LINTON WELLS, Discussant, SESSION IV

When I first looked at the themes for this afternoon's sessions, I was concerned that, between reciprocity, economic espionage and new security technology, it might be hard to find a lot of commonality. In fact, however, listening to the presentations, I am struck by the convergence.

To begin with, in all these areas, there's certainly a need for cooperation among industry, various government agencies and the public. First of all, I think government needs to begin changing a basic paradigm by realizing that we have much to learn from industry. For a long time, we've had a security system based on the presumption that classified information largely is born in the government and shared with industry, subject to severe sanctions if they mishandle the protection. Now we're finding more and more that the information that we need to know is actually originated within the private sector, and they have effective systems for protecting it. I'm sure that we'd all be better off if we learned to develop security practices with more commonality.

Second, security developments increasingly involve the Internet and other networks today, and it is important that the rules we develop incorporate domestic and government concerns as well as those which transcend national boundaries. These issues are going to be duplicated in spades in the area of encryption. I just came from a meeting on this, and in some respects the whole issue of key management and infrastructure development leads to the conclusion that reciprocity is very much equivalent to interoperability. Unless you are willing to accept the key managment certificate of someone with whom you want to communicate, you can't get there. Moreover, you don't get to that level of mutual trust without seriously talking to each other. Public and private sector dialogue is becoming more and more important since the government can't develop a security regime for the new environment by itself. We're finding that key information of importance to the individuals, and collectively to the nation, like personnel records, medical data, and logistics, don't necessarily fall under traditional headings of national security information.

The second main theme I found among the panelists' points was the need for innovation to meet the challenges of emerging areas, both in the policy and the technology realm. My deputy, Chuck Wilson, and his folks, along with DIS and their people, hosted a very interesting conference last week up in Boston on International Industrial Security in the Information Age. They had 65 people from 30 countries, many from Central and Eastern Europe, and speakers were discussing encryption, network penetration, defensive information assurance, etc. In the course of the conference, one of the European representatives commented, "I did not know you could talk to people about this subject." This just illustrates that the players, and the topics in the security area truly are changing. Many have noted that, whether via electronic techniques, or traditional document theft, the cleared insider remains a central element in all of the threat scenarios.

However, what makes us more vulnerable today is that if your network has been penetrated; there's little difference between an outsider and a cleared insider.

We also need innovation in the legislative framework. No matter how difficult and contentious that's likely to be, we have to have our laws get closer to the technology we're using. In the process, we need to consider what really is national security. When do activities of this sort threaten such a level of society's resources, or the basis of democratic process, that they in fact cause society to limit or change itself to defend against them? The distinction between sensitive and classified information also is something that we haven't dealt with as much as we should. Someone asked the other day that if, in time of crisis, the President had the choice between having to give up all the classified information available to the government or losing control of the Social Security database for a month, which would he choose? I leave it to you to judge the impact of not sending out any Social Security checks to members of senior citizens groups for a month.

At the same time, I'm encouraged by the beginning of signs of movement to a broader dialogue, such as the Security Policy Board, and the President's Commission on Critical Infastructure Protection. The latter group has been working under the Attorney General to develop ways to enhance the security of key elements of our national infrastructure, and it is on a very fast track.

However, in some cases I'm not so optimistic as some of our panelists, on three grounds. First, I don't think we can begin to see clearly now what the technology of 25 years from now will be. Certainly 25 years ago in 1971, if anyone had told us that most of us would have access to machines on our desk with computing power that probably exceed all of the core of NSA's computer center at that time, I would have been skeptical. My guess is that we'll be similarly surprised in the future.

Second, I'm not sure we're going to reach closure on some of these issues. This is a ponderous process with lots of interest groups involved. We certainly have to do extensive outreaching to try to reach as many of them as possible, but I'm not sure we'll actually get there in all cases.

And finally, I'm pessimistic on the future of the concept of "need to know." It seems to me that what's happening right now is that "need to know" is really only being applied seriously in the SAP and SCI communities. At least in the intelligence world, the focus is on getting the word out, especially below the tear line. Therefore, a secret clearance or a confidential clearance is just a secret clearance or a confidential clearance, and not many people are probing very deeply into "need to know" if you have an appropriate clearance level. I don't know how to get back from that short of changing the basic rules, which no one seems willing to do.

Nonetheless, I think the sum total of these developments suggests that the security discipline in the years ahead is going to extraordinarily exciting and dynamic. Certainly, I think the people who attended the international conference in Boston share that view. It's assuredly going to be a different time than what we've been used to.

PARTICIPANT LIST

John E. ACKERMAN
Director, Security
Harris Corporation
P.O. Box 37 M/S: 15-1120
Melbourne, FL 32902-0037
Tel: (407) 727-6050
Fax: (407) 729-1870

Thomas J. ADAMS
Manager, Information Services
Lockheed Missiles & Space Co.
1111 Lockheed Way
O/27-30, B/562
Sunnyvale, CA 94089
Tel: (408) 756-2721
Fax: (408) 742-2303

Steven AFTERGOOD (**Speaker**)
Director, Project on Government Secrecy
Federation of American Scientists
307 Massachusetts Avenue, NE
Washington, DC 20002
Tel: (202) 546-3300
Fax: (202) 675-1010

Stewart ALY
Associate Deputy General Counsel (Legal Counsel)
Office of General Counsel
1600 Defense Pentagon
Washington, DC 20301-1600
Tel: (703) 695-6804
Fax: (703) 614-6745

Maynard C. ANDERSON (**Speaker**)
President and Managing Director
Arcadia Group Worldwide, Inc.
1911 N. Fort Myer Drive, Suite 501
Arlington, VA 22209
Tel: (703) 527-9099
Fax: (703) 527-9780

Stephen F. ARGUBRIGHT, Jr.
Intelligence Officer
National Counterintelligence Center
Room 3W01 NHB
Washington, DC 20505
Tel: (703) 874-4073
Fax: (703) 874-5844

Scott R. ARMSTRONG (**Discussant**)
Executive Director
The Information Trust
2620 Quebec Street, NW
Washington, DC 20008
Tel: (202) 364-1100
Fax: (202) 364-2438

John ARQUILLA **(Speaker)**
Associate Professor
National Security Affairs
Naval Postgraduate School
Monterey, CA 93940
Tel: (408) 656-3453
Fax: (408) 656-3679

Brent N. BARRETT
Program Manager, Systems & Technologies
Naval Criminal Investigative Service
Washington Navy Yard, Bldg. 111
901 M Street, SE
Washington, DC 20388-5380
Tel: (202) 433-9405
Fax: (202) 433-9322

Lloyd BASTIAN
Security Director
IBM Corporation
1301 K Street, NW
Washington, DC 20005
Tel: (202) 515-4640
Fax: (202) 515-5088

Terry J. BATEY
Bureau Security Officer
Bureau of Alcohol, Tobacco & Firearms
US Department of the Treasury
650 Massachusetts Avenue, NW
Washington, DC 20226
Tel: (202) 927-7810
Fax: (202) 927-8585

Rosalind M. BAYBUTT
Assistant Director for Special Requirements
OASD(C3I)/ODASD(I&S)/PD(IWSCI)
Room 3C281 The Pentagon
Washington, DC 20301
Tel: (703) 695-9468
Fax: (703) 695-8215

Tom BECHERER
Research and Policy Director
Commission on Protecting and Reducing Government Secrecy
2201 C Street, NW
Room 225, SA-44
Washington, DC 20522-4402
Tel: (202) 776-8762
Fax: (202) 776-8773

C. Michael BERRY
Associate Director
Department of Defense Security Institute
8000 Jefferson Davis Highway
Richmond, VA 23297-5091
Tel: (804) 279-3813
Fax: (804) 279-5239

Nancy J. BESSLER
Instructional Technologist
Oak Ridge Institute for Science and Education
P.O. Box 117, ETD/Mitchell
Oak Ridge, TN 37932
Tel: (423) 576-1020
Fax: (423) 241-3851

Janis G. BIBEE
Facility Security Officer
Secure Computing Corporation
2675 Long Lake Road
Roseville, MN 55113
Tel: (612) 628-2748
Fax: (612) 628-2701

Eric R. BIEL **(Speaker)**
Staff Director
Commission on Protecting and Reducing Government Secrecy
2201 C Street, NW
Room 225, SA-44
Washington, DC 20522-4402
Tel: (202) 776-8758
Fax: (202) 776-8773

Mark R. J. BORSI
Director, Security Management Office
NASA Headquarters
Mail Code JLS
300 E Street, SW
Washington, DC 20546
Tel: (202) 358-0118
Fax: (202) 358-3238

Michael R. BROWN
Assistant for Information and Personnel Security
Chief of Naval Operations (NO9N2)
Building 111, Washington Navy Yard
901 M Street, SE
Washington, DC 20388-5021
Tel: (202) 433-8841
Fax: (202) 433-8849

Bruce J. CAMPBELL
Associate Director for Operations Support
Federal Emergency Management Agency
500 C Street SW, Room 525
Washington, DC 20472
Tel: (202) 646-2965
Fax: (202) 646-3155

Michael H. CAPPS
Director
Defense Polygraph Institute
Building 3165 & 13th Avenue
Fort McClellan, AL 30205-5114
Tel: (205) 848-3804
Fax: (205) 848-5332

Rusty CAPPS
Deputy Director, Center for the Study of Strategic Counterintelligence
Aegis Research Corporation
7799 Leesburg Pike, Suite 1100N
Falls Church, VA 22043
Tel: (703) 610-9296
Fax: (703) 847-5787

Ralph M. CARNEY **(PERSEREC staff)**
Program Manager
PERSEREC
99 Pacific Street, Suite 455-E
Monterey, CA 93940
Tel: (408) 656-5029
Fax: (408) 656-2041

Louis J. CARPENITO
Director, Information Security
Johnson & Johnson
1003 US Highway
Raritan, NJ 08869-0608
Tel: (908) 685-3352
Fax: (908) 685-3455

Michael G. CARTER
Assistant for Special Plans, Programs and Operations (SAF/AAZ)
SAF/Administrative Assistant for Security Oversight
1720 Air Force Pentagon
Washington, DC 22032-1720
Tel: (703) 693-2013
Fax: (703) 693-2059

James P. CHANDLER
President
National Intellectual Property Law Institute
1815 Pennsylvania Avenue, NW #300
Washington, DC 20006
Tel: (202) 842-4800
Fax: (202) 296-4098

Leigh F. CHASE
Senior Personnel Security Specialist
US Nuclear Regulatory Commission
Division of Security
Washington, DC 20555
Tel: (301) 415-6541
Fax: (301) 415-5132

Cathleen L. CIVIELLO
Psychologist
NSA/M5C1
9800 Savage Road
Fort Meade, MD 20755
Tel: (410) 859-6424
Fax: (410) 850-0833

Philip T. CLEMENT
DOD Technology Control Officer
MCI Systems Integrity
8200 Greensboro Drive
McLean, VA 22102
Tel: (703) 902-6091
Fax: (703) 902-6012

Shirley A. COFFMAN
Manager, Security & Safety Services
Lockheed Martin Technical Operations
1309 Moffett Park Drive
Sunnyvale, CA 94086
Tel: (408) 742-0323
Fax: (408) 742-4012

Bill COPE
Information Security Specialist
US Department of Transportation
Office of Security, M-70
400 7th Street, SW
Washington, DC 20590
Tel: (202) 366-4678
Fax: (202) 366-7013

Steven J. COVER
Deputy Director, Oversight
Special Programs
ODTUSD/P/PS/Special Programs
Room 3C285 The Pentagon
Washington, DC 20301
Tel: (703) 614-0578
Fax: (703) 695-4345

Shawn S. DALEY
Assistant Security Manager
Massachusetts Institute of Technology
Lincoln Laboratory
244 Wood Street
Lexington, MA 02173-9108
Tel: (617) 981-7117
Fax: (617) 981-0110

Stephanie DAMAN
First Secretary
British Embassy
3100 Massachusetts Avenue, NW
Washington, DC 20008
Tel: (202) 898-4274
Fax: (202) 898-4222

Rene DAVIS-HARDING
Deputy Director, Investigations
Defense Investigative Service
1340 Braddock Place
Alexandria, VA 22314-1651
Tel: (703) 325-5376
Fax: (703) 325-7426

James W. DEARLOVE
Senior Intelligence Officer
Office for Force Modernization (PAQ)
Defense Intelligence Agency
Washington, DC 20340-5100
Tel: (202) 231-4642
Fax: (202) 231-2711

William E. DeGENARO
President
DeGenaro & Associates, Inc.
7800 Metro Parkway, Suite 300
Bloomington, MN 55425
Tel: (612) 851-3170
Fax: (612) 851-3193

Frances B. DELKER
Manager, Personnel Security
National Security Agency
NSA, M5A, APS1, Suite 6830
Fort George G. Meade, MD 20755-6000
Tel: (410) 859-4747
Fax: (410) 684-3174

Roger P. DENK **(PERSEREC staff)**
Director
PERSEREC
99 Pacific Street, Suite 455-E
Monterey, CA 93940
Tel: (408) 656-3161
Fax: (408) 656-2041

Russell G. DeRITIS
Chief, Security Policy
OSD/Washington Headquarters Service
1155 Defense Pentagon
Washington, DC 20301-1155
Tel: (703) 695-0293
Fax: (703) 697-8333

James J. DUNLEAVY
Chief, Personnel Security Branch
US Nuclear Regulatory Commission
Division of Security
Washington, DC 20555
Tel: (301) 445-7404
Fax: (301) 415-5132

Jerry EISELE
Director
Center for Human Reliability Studies
Oak Ridge Institute for Science and Education
P.O. Box 117
Oakridge, TN 37831-0117
Tel: (423) 576-2208
Fax: (423) 576-7903

R. Lee ENGEL
Director, Security Operations
Allied Signal Technical Services Corporation
One Bendix Road
Columbia, MD 21045
Tel: (410) 964-7176
Fax: (410) 964-7181

William E. EYRES
Security Director
IBM Corporation
5600 Cottle Road
San Jose, CA 95123
Tel: (408) 256-6190
Fax: (408) 256-2138

John M. FERRONE
Manager, Personnel Security
NSA, M5A, APS1, Suite 6830
Fort George G. Meade, MD 20099-6000
Tel: (410) 859-4747
Fax: (410) 684-3174

Lynn F. FISCHER
Technical Publications Editor
Department of Defense Security Institute
8000 Jefferson Davis Highway
Richmond, VA 23297-5091
Tel: (804) 279-3824
Fax: (804) 279-6406

James A. FORSTNER
Corporate Counsel
The Dupont Company
D-40 42-2, Legal
1007 Market Street
Wilmington, DE 19898
Tel: (302) 773-0686
Fax: (302) 774-7255

Betty FRAZIER
Staffer
Security Policy Board
Suite 1101, Crystal Gateway 3
1215 Jefferson Davis Highway
Arlington, VA 22202
Tel: (703) 602-6997
Fax: (703) 602-7209

Stephen E. GARMON
Director of Security
US Department of Commerce
Room 5039
14th and Constitution Avenue, NW
Washington, DC 20230
Tel: (202) 482-4371
Fax: (202) 501-6355

Dorothy R. GARRISON
Personnel Security Program Manager
Defense Mapping Agency
8613 Lee Highway
Fairfax, VA 22031-2137
Tel: (703) 275-8346
Fax: (703) 275-5759

Dan GARWICK
Security Manger
Rockwell Aerospace
12214 Lakewood Boulevard (DA 18)
Downey, CA 90241
Tel: (310) 922-3104
Fax: (310) 922-2155

Kenneth GEIDE **(Speaker)**
Unit Chief, Economic Espionage
Federal Bureau of Investigations
Room 4448
935 Pennsylvania Avenue, NW
Washington, DC 20535-0001
Tel: (202) 324-8462
Fax: (202) 324-4764

William F. GIESE
Group Manager, Security
McDonnell Douglas Corporation
Mail Code 102 2043
P.O. Box 516
St. Louis, MO 63166
Tel: (314) 232-3348
Fax: (314) 234-2340

Gary H. GOWER
Senior Professional Staff
Commission on Protecting and Reducing Government Secrecy
2201 C Street, NW
Room 225 SA-44
Washington, DC 20522-4402
Tel: (202) 776-8752
Fax: (202) 776-8773

Mary H. GRIGGS
NACIC Officer
National Counterintelligence Center
3W01 NHB
Washington, DC 20505
Tel: (703) 874-5544
Fax: (703) 874-5929

Gregory A. GWASH
Director for Industrial Security
Defense Investigative Service
1340 Braddock Place
Alexandria, VA 11214-1651
Tel: (703) 325-5277
Fax: (703) 325-7426

David R. A. HAAG
Chief, Security Policy Center
Central Intelligence Agency
DA/OPS/SPC
Washington, DC 20505
Tel: (703) 482-5345
Fax: (703) 482-0353

Martin V. HALE
Deputy Director (Counterintelligence)
On-Site Inspection Agency
201 W. Service Road
Dulles International Airport
Washington, DC 20041-0498
Tel: (703) 810-4446
Fax: (703) 810-4343

John HANCOCK
Senior Professional Staff
Commission on Protecting and Reducing Government Secrecy
2201 C Street, NW
SA-44, Room 225
Washington, DC 20522-4402
Tel: (202) 776-8737
Fax: (202) 775-8773

Dennis HANRATTY
Staffer
Security Policy Board
Suite 1101, Crystal Gateway 3
1215 Jefferson Davis Highway
Arlington, VA 22202
Tel: (703) 602-6997
Fax: (703) 602-7209

Gary HARRIS
Staffer
Security Policy Board
Suite 1101, Crystal Gateway 3
1215 Jefferson Davis Highway
Arlington, VA 22202
Tel: (703) 602-6997
Fax: (703) 602-7209

Mark R. HEILBRUN
Counsel
Senate Select Committee on Intelligence
HART 211 (Senate)
Washington, DC 20510
Tel: (202) 224-4358
Fax: (202) 224-1772

Seymour M. HERSH **(Speaker)**
Journalist
1211 Connecticut Avenue, NW
Suite 320
Washington, DC 20036
Tel: (202) 872-0703
Fax: (202) 872-0705

Charles J. HEUBUSCH
Safeguards & Security Programs Coordinator
US Department of Energy, S&S Central Training Academy
19901 Germantown Road
Germantown, MD 20874
Tel: (301) 903-5439
Fax: (301) 903-2054

Joe HOLTHAUS
Staffer
Security Policy Board
Suite 1101, Crystal Gateway 3
1215 Jefferson Davis Highway
Arlington, VA 22202
Tel: (703) 602-6997
Fax: (703) 602-7209

Joseph J. HORVAT
Manager, Security & Fire Protection, DC Office
The Boeing Company
7990 Boeing Court
MS CV-43
Vienna, VA 22182
Tel: (703) 903-1531
Fax: (703) 903-1530

Emilio JAKSETIC
Chairman, Appeal Board
DLSA/Defense Office of Hearings and Appeals
P.O. Box 3656
Arlington, VA 22203-1995
Tel: (703) 696-4759
Fax: (703) 696-6865

Scott H. JOHNSON
Director, Program Integrity Division
US Department of the Treasury/Financial Management
401 14th Street, SW Room 222
Washington, DC 20227
Tel: (202) 874-7050
Fax: (202) 874-7292

David B. KENDRICK
Manager, DISP
E-Systems Inc., Garland Division
MS: FB93200
P.O. Box 660023
Dallas, TX 75266-0023
Tel: (214) 205-5776
Fax: (214) 205-7347

Robert J. KETTERING
Manager, Security
McDonnell Douglas Corporation
Mail Code 102 2043
P.O. Box 516
St. Louis, MO 63166
Tel: (314) 233.8111
Fax: (314) 234-2340

Milton R. KIRSTE
Security Manager
MIT Lincoln Laboratory
244 Wood Street
Lexington, MA 02173-9108
Tel: (617) 981-7112
Fax: (617) 981-0110

Catherine M. KISER
Special Agent/FBI
National Counterintelligence Center
Room 3W01 NHB
Washington, DC 20505
Tel: (703) 874-4078
Fax: (703) 874-5844

Michael A. KRAYNICK
Manager, Personnel Security
National Security Agency
NSA, M5A, APS1, Suite 6830
Fort George G. Meade, MD 20755-6000
Tel: (410) 859-6601
Fax: (410) 684-3174

Shirley E. KRIEGER
Director, Support Services
Honeywell, Inc.
Satellite Systems Operations
P.O. Box 52199
Phoenix, AZ 85072-2199
Tel: (602) 561-3271
Fax: (602) 561-3190

Michael R. LAMB
Chief, Information Warfare Support Division
Defense Intelligence Agency
Attn: PGI-5
Washington, DC 20340
Tel: (202) 231-4094
Fax: (202) 231-4199

Bernie LAMOUREUX
Lockheed Martin Corporation
6801 Rockledge Drive
Bethesda, MD 20817
Tel: (301) 897-6271
Fax: (301) 897-6083

Raymond F. LEAVITT, Jr.
Director, Corporate Security
The MITRE Corporation
202 Burlington Road
Bedford, MA 01730
Tel: (617) 271-7641
Fax: (617) 271-8843

Maureen LENIHAN
Research Associate
Commission on Protecting and Reducing Government Secrecy
2201 C Street, NW
Room 225 SA-44
Washington, DC 20522-4402
Tel: (202) 776-8733
Fax: (202) 776-8773

Art LESSER
President
Merit Security
2825 El Camino Real
Redwood City, CA 94061
Tel: (415) 366-0100
Fax: (415) 366-7530

Harry LETAW Jr. (**Speaker**)
Chairman and CEO
Essex Corporation
9150 Guilford Road
Columbia, MD 21046
Tel: (301) 953-8830
Fax: (301) 953-7880

Donald M. LE VINE
Principal Engineer
Defense Nuclear Agency
Springfield Research Facility
5400 Port Royal Road
Springfield, VA 22151-2301
Tel: (703) 321-0008
Fax: (703) 321-7521

James R. LINNEN
Chief, CI/Security/IW
OASD/CISA
1215 Jefferson Davis Highway
Suite 1101
Arlington, VA 22202
Tel: (703) 602-5038
Fax: (703) 602-5890

James A. LONG
Acting Department Security Officer
US Department of Agriculture
Room 18 West
14th and Independence Avenue, SW
Washington, DC 20250-9616
Tel: (202) 720-8313
Fax: (202) 690-0681

Jerry B. LYONS
CI Analyst
NACIC/TAO
Central Intelligence Agency
Washington, DC 20505
Tel: (703) 874-3268
Fax: (703) 874-5844

John F. MALLON
Chairman of the Board
ASIS
One Johnson & Johnson Plaza
New Brunswick, NJ 08933
Tel: (908) 524-3272
Fax: (908) 524-6687

Peter K. MANNING (**Speaker**)
Professor of Sociology and Criminal Justice
School of Criminal Justice
560 Baker Hall
Michigan State University
East Lansing, MI 48824-1118
Tel: (517) 355-2199
Fax: (517) 432-1787

Renee M. MAXWELL
Security Policy Officer
Central Intelligence Agency
Washington, DC 20505
Tel: (703) 482-5345
Fax: (703) 734-1283

Jim McCARTY
Analyst
GRCI
1900 Gallows Road
Vienna, VA
Tel: (703) 506-5771
Fax: (703) 356-5727

Daniel A. McGARVEY
National Reconnaissance Office
14675 Lee Road
Chantilly, VA 22021-1715
Tel: (703) 808-3633
Fax: (703) 222-7832

Robert A. McMENAMIN
Assistant Director (Physical Security)
US Department of the Treasury
1500 Pennsylvania Avenue, NW #1306
Washington, DC 20220
Tel: (202) 622-1120
Fax: (202) 622-1056

Michael H. McMILLAN
Chief, Security Office
On-Site Inspection Agency, DOD
201 W. Service Road
P.O. Box 17498
Washington, DC 20041-0498
Tel: (703) 810-4384
Fax: (703) 810-4098

William MEEHAN
Assistant Director, Office of Intelligence
U.S. Customs Service
1301 Constitution Avenue, NW
Washington, DC 20229
Tel: 202) 927-0330
Fax: (202) 927-1738

John W. MOONEY
Chief, Personnel Security, Departmental Offices
US Department of the Treasury
1500 Pennsylvania Ave NW Room 1322
Washington, DC 20220
Tel: (202) 622-1112
Fax: (202) 622-2429

MG John E. MORRISON, JR. USAF (Ret.)
Executive Vice President
Security Affairs Support Association
141 National Business Parkway, #112
Annapolis Junction, MD 20701
Tel: (301) 470-4445
Fax: (301) 604-6413

Rowland A. MORROW
Consultant
DCI/CSE
3701 St. Paul Street
Baltimore, MD 21218
Tel: (202) 596-5169
Fax: (202) 496-2588

Senator Daniel Patrick MOYNIHAN
(Invited Speaker)
Chairman
Commission on Protecting and Reducing Government Secrecy
2201 C Street, NW Room 225 SA-44
Washington, DC 20522-4402
Tel: (202) 776-8758 (Commission)
Fax: (202) 776- 8773 (Commission)

Margaret R. MUNSON
Director
Defense Investigative Service
1340 Braddock Place
Alexandria, VA 22314-1651
Tel: (703) 325-5308
Fax: (703) 325-3619

R. Gary MYERS
Director of Corporate Security
SRI
333 Ravenswood Avenue
Menlo Park, CA 94025
Tel: (415) 859-3875
Fax: (415) 859-5766

Peter NELSON
Deputy for Personnel Security
Room 3C267 The Pentagon
Washington, DC 20301
Tex: (703) 697-3039
Fax: (703) 695-8215

William O'CONNELL
Central Intelligence Agency
Washington, DC 20505
Tel: (703) 482-0820
Fax: (703) 482-8515

Arthur W. O'CONNOR
Security Manager
GTE Electronic Defense Systems
Division
GTE Government Systems Corporation
1700 Research Boulevard
Rockville, MD 20850-3181
Tel: (301) 738-8950
Fax: (301) 294-8652

Richard P. O'NEILL
Captain, US Navy
Office of the Assistant Secretary of
Defense (C3I)
Room 3D200 The Pentagon
Washington, DC 20301-6000
Tel: (703) 614-0625
Fax: (703) 614-0627

Robert J. OPFER
Security Programs Manager
Federal Bureau of Investigations
935 Pennsylvania Avenue, NW
Room 4246
Washington, DC 20535
Tel: (202) 324-4901
Fax: (202) 324-4973

Stafford W. OUDERKIRK
Deputy Director
DOD, IUSD(P&R),
ASD(FMP)(MPP)AP
Room 2B271 The Pentagon
Washington, DC 20301-4000
Tel: (703) 695-5525
Fax: (703) 614-9272

Cary PAGE
Planning Officer, ADDA/IS Staff
Central Intelligence Agency
Washington, DC 20505
Tel: (703) 482-0820
Fax: (703) 482-8515

Emmett PAIGE, Jr. (**Keynote Speaker**)
Assistant Secretary of Defense, C3I
Room 3E172 The Pentagon
Washington, DC 20301
Tel: (703) 695-0348
Fax: (703) 614-8060

Greg PANNONI
Staffer
Security Policy Board
Suite 1101, Crystal Gateway 3
1215 Jefferson Davis Highway
Arlington, VA 22202
Tel: (703) 602-6997
Fax: (703) 602-7209

A. L. PAPENFUS
Director, Personnel and Security
Washington Headquarters Service
1155 Defense Pentagon
Washington, DC 20301-1155
Tel: (703) 697-1703
Fax: (703) 697-8333

Peggi A. PARKS
Security Director
HDS, Inc.
12310 Pincecrest Road
Reston, VA 22091
Tel: (703) 620-6200
Fax: (703) 620-3169

James D. PASSARELLI
Staff Member
Security Policy Board
Suite 1101, Crystal Gateway 3
1215 Jefferson Davis Highway
Arlington, VA 22202
Tel: (703) 602-9981
Fax: (703) 602-7209

Victor K. PATRICK
Chief, Security Operation Division
DISA/CISS
5113 Leesburg Pike, Suite 400
Falls Church, VA 22041
Tel: (703) 681-7972
Fax: (703) 681-5756

Douglas G. PERRITT, Sr.
Principal Director, Information
Warfare,Security and
Counterintelligence
OASD(C3I)/ODASD(I&S)
Washington, DC 20301-6000
Tel: (703) 695-6609
Fax: (703) 695-8215

Herbert D. POND
Director of Security
Lockheed Martin Vought Systems
P.O. Box 650003
Dallas, TX 75265-0003
Tel: (214) 603-9745
Fax: (214) 603-1508

Lee A. PRIVETT
Deputy Director, Office of Security
US Department of Transportation
400 7th Street, SW Room 7402
Washington, DC 20590
Tel: (202) 366-4677
Fax: (202) 366-7013

Sharon F. REINKE
Chief, Navy Division
Office of Assistant Secretary of Defense
(Public Affairs)
Directorate for Freedom of Information
and Security Review
1400 Defense Pentagon
Washington, DC 20301-1400
Tel: (703) 697-2716
Fax: (703) 693-7341

Joseph P. REYNOLDS
Director, Security
Sanders, A Lockheed Martin Company
P.O. Box 868
Nashua, NH 03061-0868
Tel: (603) 885-5514
Fax: (603) 885-3178

James A. RIEDEL **(PERSEREC staff)**
Deputy Director
PERSEREC
99 Pacific Street, Suite 455-E
Monterey, CA 93940
Tel: (408) 656-5026
Fax: (408) 656-2041

Robert B. RITTER
OPSEC Officer
Interagency OPSEC Support Staff
6411 Ivy Lane #400
Greenbelt, MD 20770-1405
Tel: (301) 982-0724
Fax: (301) 982-2913

Joanne B. ROTH
Senior Security Administrator
AlliedSignal Technical Services
Corporation
One Bendix Road
Columbia, MD 21045
Tel: (410) 964-7173
Fax: (410) 964-7181

Jerry RUBINO
Director, Security & Emergency Planning
US Department of Justice
10th & Pennsylvania Avenue, NW
Washington, DC 20530
Tel: (202) 514-2094
Fax: (202) 307-2069

Peter SADERHOLM **(Speaker)**
Director
Security Policy Board Staff
Suite 1101, Crystal Gateway 3
1215 Jefferson Davis Highway
Arlington, VA 22202
Tel: (703) 602-9988
Fax: (703) 602-7209

Robert B. SAFREED
Director, Corporate Security
AlliedSignal Inc.
2525 West 190th Street
Torrance, CA 90504
Tel: (310) 512-1193
Fax: (310) 512-1973

Marshall C. SANDERS
TASC Systems Division
12100 Sunset Hills Road
Reston, VA 22090
Tel: (703) 834-5024
Fax: (703) 318-7900

Theodore R. SARBIN **(PERSEREC staff)**
Research Pyschologist
PERSEREC
99 Pacific Street, Suite 455-E
Monterey, CA 93940
Tel: (408) 656-5030
Fax: (408) 656-2041

Leon J. SCHACHTER
Director
Defense Office of Hearings and Appeal
4015 Wilson Boulevard, Suite 300
Arlington, VA 22203
Tel: (703) 696-4598
Fax: (703) 696-6865

G. Dan SMITH **(Speaker)**
Program Manager, Technology Development
Department of Energy
NN513
19901 Germantown Road
Germantown, MD 20874
Tel: (301) 903-2545
Fax: (301) 903-4164

John T. SMITH
FMS Security Officer
Financial Management Service
US Department of the Treasury
3700 East-West Highway, #163B
Hyattsville, MD 20782
Tel: (202) 874-7030
Fax: (202) 874-8682

Michael P. STEPHENS
Chief, Office of Security
Bureau of Engraving and Printing
14th & C Streets, SW Room 510A
Washington, DC 20228
Tel: (202) 874-3647
Fax: (202) 874-3614

Coby STOHRER
Assistant Director (Personnel Security)
US Department of the Treasury
1500 Pennsylvania Avenue, NW
Washington, DC 20220
Tel: (202) 622-1120
Fax: (202) 622-1056

Ethel R. THEIS **(Discussant)**
Associate Director
Information Security Oversight Office
750 17th Street, NW, Suite 530
Washington, DC 20006
Tel: (202) 219-5385
Fax: (202) 219-5250

Terry THOMPSON
Staffer
Security Policy Board
Suite 1101, Crystal Gateway 3
1215 Jefferson Davis Highway
Arlington, VA 22202
Tel: (703) 602-6997
Fax: (703) 602-7209

Alvin A. ULSH III
Director, Security
Lockheed Martin Tactical Systems
9500 Godwin Drive
Manassas, VA 22110
Tel: (703) 367-6504
Fax: (703) 367-1131

Michele VAN CLEAVE **(Discussant)**
Attorney
Feith and Zell
2300 M Street, NW Suite 600
Washington, DC 20037
Tel: (202) 293-1600
Fax: (202) 293-8965

Tina VAUGHEN
Manager, Protection Technologies & Services
BDM Federal
20300 Century Boulevard, Suite 173
Germantown, MD 20874
Tel: (301) 601-5504
Fax: (301) 601-5505

Harry VOLZ
Consultant
64 Linden Street
Massapequa Park, NY 11762-1008
Tel: (516) 541-5517
Fax: (516) 541-5517

Lorraine T. WAGER
Security Policy Officer
Central Intelligence Agency
Washington, DC 20505
Tel: (703) 482-5345
Fax: (703) 482-0353

Michael J. WAGUESPACK
Director
National Counterintelligence Center
Room 3W01 New HQ Building
Washington, DC 20505
Tel: (703) 874-4117
Fax: (703) 874-5844

Murray B. (Scotty) WATT
Lockheed-Martin Technical Operations
131 National Business Parkway, Suite 220
Annapolis Junction, MD 21144
Tel: (301) 497-9466
Fax: (301) 497-2202

Linton WELLS II **(Discussant)**
Deputy to the Under Secretary of Defense for Policy Support
Room 2E812 The Pentagon
Washington, DC 20301
Tel: (703) 697-0286
Fax: (703) 614-8976

Carl M. WHERRY
Security Manager
Lockheed Martin Corporation
Crystal Square 2, Suite #300
1725 Jefferson Davis Highway
Arlington, VA 22202
Tel: (703) 413-5802
Fax: (703) 413-5819

Eugene J. WHITE
Director, Information Security
HQ USAF/SPI
1340 Air Force Pentagon
Washington, DC 20330-1340
Tel: (703) 588-0007
Fax: (703) 588-0035

Larry D. WILCHER
Program Manager, Technical and Operations Security
US Department of Energy NN-5123
19901 Germantown Road
Germantown, MD 20874
Tel: (301) 903-2528
Fax: (301) 903-8717

Claudell WILLIAMS
Corporate Director, Security
GRC International, Inc.
1900 Gallows Road
Vienna, VA 22182
Tel: (703) 506-5558
Fax: (703) 356-5727

Charles C. WILSON, Jr.
Asstant Deputy to the USD(P) for Policy Support
OSD/OUSD(P)
Room 2E812 The Pentagon
2000 Defense Pentagon
Washington, DC 20301-2200
Tel: (703) 695-6607
Fax: (703) 614-8976

Martin F. WISKOFF (**PERSEREC contractor**)
Senior Scientist
BDM Federal, Inc.
99 Pacific Street, Suite 455-E
Monterey, CA 93940
Tel: (408) 656-5020
Fax: (408) 656-2041

H. Allen WITZGALL
Unit Chief
Federal Bureau of Investigations
10th & Pennsylvania Avenue, NW
Washington, DC 20535
Tel: (202) 324-4905
Fax: (202) 324-8524

Calvin A. WOOD
Deputy Director
Interagency OPSEC Support Staff
6411 Ivy Lane, Suite 400
Greenbelt, MD 20770
Tel: (301) 982-2313
Fax: (301) 982-2913

Suzanne WOOD (**PERSEREC staff**)
Project Manager
PERSEREC
99 Pacific Street, Suite 455-E
Monterey, CA 93940
Tel: (408) 656-5025
Fax: (408) 656-2041

Charleen WRIGHT
Assistant Director for Personnel Security (Research & Special Projects)
OASD(C3I)
6000 Defense Pentagon, Room 3C281
Washington, DC 20301-6000
Tel: (703) 697-3039
Fax: (703) 695-8215